PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-319339

(43)Date of publication of application : 16.11.2001

---

(51)Int.Cl. G11B 7/005
G06F 12/14
G11B 19/02
G11B 20/10

---

(21)Application number : 2000-138346 (71)Applicant : TAIYO YUDEN CO LTD

(22)Date of filing : 11.05.2000 (72)Inventor : OMURA YUKIHIDE
SUNAKAWA RYUICHI
SHIMIZU HIRONOBU

---

# (54) WRITE ONCE TYPE OPTICAL DISK AND RECORDING AND REPRODUCING DEVICE AND RECORDING MEDIUM FOR THE OPTICAL DISK

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the illegal readout of the recorded information of a write once type optical disk.

SOLUTION: In the write once type optical disk provided with a user area for writing user data and a system area to be used by a system at least when the pertinent writing operation is performed, information for a security measure is written on a part of the system area of the optical disk and the disk is shipped. Since the disk is shipped while the information for the security measure written in the system area are in a invisible

state for a user, the information are hidden from the user, the illegal readout of the recorded information is prevented by utilizing these hidden information.

---

LEGAL STATUS [Date of request for examination] 02.10.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3871851
[Date of registration] 27.10.2006
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]



---

CLAIMS

---

[Claim(s)]

[Claim 1] The write-once mold optical disk characterized by writing the information for security countermeasures in said a part of system area, and making it ship to it in the write-once mold optical disk equipped with the user area for writing in user data, and the system area used by the system in case the write-in actuation concerned is performed at least.

[Claim 2] Said system area is a write-once mold optical disk according to claim 1 characterized by being a field for laser on-the-strength calibrations at the time of writing in user data.

[Claim 3] Said system area is a write-once mold optical disk according to claim 1 characterized by being either of the fields for specifying the termination location of the field for session information storing referred to in case the user data written in the field for temporary storages of the session information at the time of writing in user data or the user area are reproduced, or a user area.

[Claim 4] The information for said security countermeasures is a write-once mold optical disk according to claim 1 characterized by being the identification information for user authentication.

[Claim 5] The information for said security countermeasures is a write-once mold optical disk according to claim 1 characterized by being the key information for enciphering said user data.

[Claim 6] The information for said security countermeasures is a write-once mold optical disk according to claim 1 characterized by being the key information for decoding the encryption data written in said user area.

[Claim 7] An access means to access the write-once mold optical disk with which the information for security countermeasures was written in a part of system area, An authentication means to judge coincidence with the authentication information inputted from the information and the outside for said security countermeasures read by said access means, and to perform user authentication, The record regenerative apparatus for write-once mold optical disks characterized by having a permissible means to permit access from the outside to said write-once mold optical disk when a registered user's authentication is performed by said authentication means.

[Claim 8] An access means to access the write-once mold optical disk with which the information for security countermeasures was written in a part of system area, An authentication means to judge coincidence with the authentication information inputted from the information and the outside for said security countermeasures read by said access means, and to perform user authentication, The record medium

characterized by storing the program for realizing a permissible means to permit access from the outside to said write-once mold optical disk when a registered user's authentication is performed by said authentication means.

---

DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the record regenerative apparatus for a write-once mold optical disk and write-once mold optical disks, and a record medium. It is related with the record regenerative apparatus for a write-once mold optical disk and write-once mold optical disks and record medium which are represented in detail by CD-R (Compact Disc Recordable) which can write in data only once.

[0002]

[Description of the Prior Art] As a distribution medium of electronic data, such as various contents and a computer program, CD-ROM (Compact Disc Read Only Memory) is used abundantly. Although CD-ROM is the by-product manufactured by press molding etc. from the master CD which recorded electronic data and it is mainly used for the media of extensive distribution, the optical disk unit of a write-once mold, i.e., CD-R, is used for little sample version CD and private CD of the number of distribution (the number of manufactures). CD-R has the difference in CD-ROM and

structure between transparent disk substrates and reflecting layers (detailed structure is mentioned later.) in that it has the recording layer which consists of organic coloring matter, irradiates high power laser at the recording layer concerned using the recording device (CD-R writer) of dedication, and can record information in a user phase by forming an information pit in the recording layer concerned by the thermal reaction.

[0003] CD-R is the write-once (postscript is possible) mold which cannot perform informational elimination or overwrite as above-mentioned. That is, informational elimination and informational rewriting which were written in once are impossible. Therefore, it is a storage indispensable to applications, such as distribution of electronic data which requires especially maintenance, and storage, from having the outstanding advantage that informational elimination and the informational alteration by the inaccurate person can be prevented certainly.

[0004]

[Problem(s) to be Solved by the Invention] However, if it was in the conventional write-once mold optical disk, although there was an outstanding advantage that elimination and an alteration of recording information could be prevented, since read-out of recording information was free, there was un-arranging [ that unjust read-out or the illegal copy of recording information could not be prevented ]. For this reason, storage of CD-R which recorded the information which requires secrecy is faced. Although a strict management regulation must be applied, employment of such a management regulation is considerable difficulty. As a result of in many cases being easy to flow in an easy inclination and being able to prevent carrying out of CD-R and read-out of information by the indiscreet person neither from the inconsistency of a regulation, nor tameness, there was a trouble that the external outflow of the information which should be kept secret, or the appearance of CD-R copied unjustly was nonavoidable.

[0005] In addition, although this trouble is being able to say the general storage device of not only CD-R but a portable mold, it is serious about especially CD-R. Actually, in addition, CD-R is because unjust reading of the recording information is possible also even for after no more use, unless CD-R which is widely used for distribution, storage, etc. of electronic data which require maintenance taking advantage of the write-once type of the description and which became unnecessary is destroyed physically (for example, a blemish is given or cut intentionally).

[0006] therefore, the technical problem which this invention tends to solve -- unjust read-out of the recording information of a write-once mold optical disk -- preventing

-- with -- **** -- it is in offering the write-once mold optical disk which suits applications, such as distribution of electronic data which requires especially maintenance, and storage.

[0007]

[Means for Solving the Problem] A write-once mold optical disk according to claim 1 is characterized by writing the information for security countermeasures in said a part of system area, and making it ship to it in the write-once mold optical disk equipped with the user area for writing in user data, and the system area used by the system in case the write-in actuation concerned is performed at least. According to this, the information for the security countermeasures written in the system area maintains the invisible condition from a user, and is shipped.

[0008] A write-once mold optical disk according to claim 2 is characterized by said system area being a field for laser on-the-strength calibrations at the time of writing in user data in a write-once mold optical disk according to claim 1. According to this, the information for security countermeasures is written in and shipped to the specific field (field for laser on-the-strength calibrations) to which the existence is disregarded at the time of playback of data.

[0009] A write-once mold optical disk according to claim 3 is characterized by said system area being either of the fields for specifying the termination location of the field for session information storing referred to in case the user data written in the field for temporary storages of the session information at the time of writing in user data or the user area are reproduced, or a user area in a write-once mold optical disk according to claim 1. According to this, the information for security countermeasures is written in the field to which direct access from a user is not permitted, and all are shipped to it.

[0010] A write-once mold optical disk according to claim 4 is characterized by the information for said security countermeasures being the identification information for user authentication in a write-once mold optical disk according to claim 1. According to this, the user authentication using the information for security countermeasures becomes possible in a user phase.

[0011] A write-once mold optical disk according to claim 5 is characterized by the information for said security countermeasures being the key information for enciphering said user data in a write-once mold optical disk according to claim 1. According to this, the user data encryption using the information for security countermeasures becomes possible in a user phase.

[0012] A write-once mold optical disk according to claim 6 is characterized by the

information for said security countermeasures being the key information for decoding the encryption data written in said user area in a write-once mold optical disk according to claim 1. According to this, the decode using the information for security countermeasures of encryption data is attained in a user phase.

[0013] The record regenerative apparatus for write-once mold optical disks according to claim 7 An access means to access the write-once mold optical disk with which the information for security countermeasures was written in a part of system area, An authentication means to judge coincidence with the authentication information inputted from the information and the outside for said security countermeasures read by said access means, and to perform user authentication, When a registered user's authentication is performed by said authentication means, it is characterized by having a permissible means to permit access from the outside to said write-once mold optical disk. According to this, by loading with the write-once mold optical disk with which the information for security countermeasures was written in a part of system area, and using the information for the security countermeasures, authentication processing of a registered user is attained, for example, data logging to said write-once mold optical disk and the security in the case of the data playback from said write-once mold optical disk are secured.

[0014] An access means by which a record medium according to claim 8 accesses the write-once mold optical disk with which the information for security countermeasures was written in a part of system area, An authentication means to judge coincidence with the authentication information inputted from the information and the outside for said security countermeasures read by said access means, and to perform user authentication, When a registered user's authentication is performed by said authentication means, it is characterized by storing the program for realizing a permissible means to permit access from the outside to said write-once mold optical disk. According to this, said access means, an authentication means, and a permissible means are realized by organic association with the hardware property and this program containing a microcomputer.

[0015]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained to a detail with reference to a drawing. In addition, instantiation of the notation of the specification thru/or example and numeric value of various details in the following explanation, or a character string and others is reference to the last for making thought of this invention clear, and it is clear that its the thought of this invention is not limited by those all or parts. Moreover, although the explanation

covering the details is avoided about the well-known technique, a well-known procedure, well-known architecture, and well-known circuitry (following "common knowledge matter"), this is also for giving explanation brief and does not eliminate intentionally all or a part of these Governor Shu term. Since it is this the Shu Governor term at the application time of this invention and this contractor can just be going to know it, naturally it is contained in the following explanation.

[0016] Drawing 1 is the external view (a) and its important section enlarged drawing (b) of a write-once mold optical disk (henceforth "CD-R"). Setting to these drawings, CD-R1 is the diameter of 12cm (there is also a thing with a diameter of 8cm.). Hereafter, it is a thing with a diameter of 12cm and explains. It has the shape of a disk and with a diameter of 15mm center hall 1a is formed in the core of a disk. The distance from the core T0 of a disk to the wall (disk common-law marriage T1) of center hole 1a 7.5mm, The distance from T0 to the disk rim T7 is 60mm. Among these T1-T7 Two or more concentric record sections, That is, they are PCA (Power Calibration Area), PMA (Program Memory Area), and a lead-in groove (it has abbreviated to "RI" by a diagram.) to the order from the inner circumference side of a disk. Data area (it has abbreviated to "UA" by a diagram.) And lead-out (it has abbreviated to "RO" by a diagram.) Each field is prepared.

[0017] When each field is outlined, PCA located in T2 - T3 is a trial writing field for the laser adjustment on the strength performed in case data are recorded on CD-R1. Generally about 100 times of this trial writing are possible, and it consumes the field of one batch by at least 1 time of data logging. PMA located in T3 - T four is a field where the track number and initiation/termination location are saved temporarily, when there is a truck of the session which is not closed yet by CD-R1. The lead-in groove (RI) located in T-four-T5 is a field in the head (inner circumference side of a disk) of a session truck, and is a field where TOC (the number of trucks currently recorded on Table Of Contents:CD, a starting position, and the die length of the sum total of a data area) of a session is saved. A closing of a session writes the information saved at PMA temporarily in this lead-in groove (RI).

[0018] The data area (UA) located in T5-T6 is a field in which data are actually written in a user phase. The storage capacity of data is about 680 M bytes (a thing with a diameter of 8cm is about 190 M bytes of max) of max, and if this storage capacity is expressed with sound recording time amount, it will become in the maximum about 74 minutes (a thing with a diameter of 8cm is the maximum about 21 minutes). a data area (UA) is managed by the logical block of the predetermined size (2 K bytes) unit which continues from immediately the back of a lead-in groove (RI) -- having --

coming -- **** -- every logical block -- the max from 0 -- LBN (Logical Block Number) to about 330000 is assigned. The lead-out (RO) located in T6-T7 is a field in the last (periphery side of a disk) of a session, and is a field which shows that the last of a data area (UA) was reached.

[0019] The location on the disk of each [ these ] field is standardized except for T2 and T3. That is, the location where T four separated from T0 23mm, the location where T5 separated from T0 25mm, and T6 are prescribed to become the location distant from T0 58mm. In addition, this is the convenience of illustration although the same sign (T7) shows the disk rim and the termination location of lead-out (RO) by a diagram. The actual termination location of lead-out (RO) turns into a location distant from T0 58.5mm. The following, as long as there is no notice, T7 shall express the termination location of lead-out (RO). In addition, initiation and the termination location (T6 and T7) of lead-out (RO) change according to the amount of the data recorded on CD-R1. The above-mentioned actual value (T6=58mm, T7=58.5mm) is a thing when making the amount of stored data into max.

[0020] Drawing 2 is cross-section structural drawing of CD-R1. CD-R1 is transparent, and on substrate 1b which consists of an ingredient (for example, plastics) which was excellent in thermal resistance, moisture resistance, and a moldability, and was equipped with necessary optical properties (a refractive index, birefringence, etc.), the laminating of the protective layer 1e which consists of hard material, such as 1d of reflecting layers, resin, etc. which consist of metallic materials, such as recording layer 1c which consists of organic coloring matter, and aluminum, is carried out, it is formed, and the thickness of the whole cross section is 1.2mm

[0021] The point that the point of having recording layer 1c, and 1f of spiral guide rails called a wobbles groove between recording layer 1c and substrate 1b are formed has the difference in structure with CD-ROM. Record of the data to CD-R1 irradiates the powerful laser for record along with 1f of guide rails from the background of substrate 1b, and is performed by heating recording layer 1c and forming an information pit (pit: a part for the physical deformation affected zone for modulating the laser reflected light for playback).

[0022] Drawing 3 is the format conceptual diagram of each record section of CD-R1. In this drawing, PCA, PMA, a lead-in groove (RI), a data area (UA), and lead-out (RO) correspond to the same name part in drawing 1 (b), respectively. Although the size (information write-in possible capacity) of PCA and PMA is not fixed, differ for every manufacturer, about 3.5 M bytes is secured by the initial complement corresponding to the above-mentioned count of trial writing (generally about 100 times), or the count

of temporary storage of session information, for example, PCA, and the capacity of about 2 M bytes is secured by PMA. Incidentally, the starting position (T2) of PCA and the starting position (T3) of PMA can be expressed in writing from such instantiation capacity with the location for "T2=T-four-about 35 seconds", and the location for "T3=T-four-about 13 seconds" on the basis of the starting position (T four) of the standardized lead-in groove (RI).

[0023] As stated above, the trial writing field at the time of PCA performing data logging and PMA are fields which store temporarily the session information which is not closed, and these two fields (PCA/PMA) are fields used only at the time of data logging (access). On the other hand, the field where data are actually written in, and the lead-out (RO) of the field which records as TOC the session information by which the lead-in groove (RI) was closed, and a data area (UA) are fields which specify the end of a data area, and these three fields (a lead-in groove / data area / lead-out) are fields used at both times of data logging and playback (access).

[0024] On the other hand, if all these fields are seen in respect of the access ease from a user that is The reader of CD-R1 If it evaluates in respect of the ability of the contents of storage to be easily accessed using the usual tools (file system on the operating system typically carried in the personal computer concerned etc.) from users, such as a personal computer which it had Although complete grasp of the contents of storage is possible though natural about a data area (UA), contents grasp of other fields (PCA, PMA, a lead-in groove, and lead-out) is impossible.

[0025] Of course, since such a tool is difficult to receive for a general user, if it is possible if a special tool is used, but use of the exceptional tool to apply is removed, it can be said that other fields other than a data area (PCA, PMA, a lead-in groove, and lead-out) are special fields where only access from a system was permitted. Hereafter, this special field is called "system area" and the thing of the field where access from a user was permitted is made a "user area." That is, a user area, other PCA, PMA, a lead-in groove (RI), and lead-out (RO) of a data area (UA) are system areas.

[0026] Now, the description of CD-R1 in the gestalt of this operation is that it writes the proper information on CD-R1 (henceforth "ID information"), and predetermined cryptographic key information in a part of system area at the time of manufacture. Although it is desirable to have a unique value (value not overlapping) covering the total number of manufactures of CD-R1 as for ID information, since there is concern whose information bit forms many bits and presses the storage capacity of a system area when the number of manufactures becomes huge, it is good also as different information for every manufacture lot, every production line, and every manufacture

stage.

[0027] This ID information is used for access collating to CD-R1 in a user phase so that it may mention later. The input of ID is required with the application which reproduces data, coincidence with inputted ID and ID currently written in the system area is judged, and, only in coincidence, access is permitted. The playback and the duplicate of data by the inaccurate user (user who does not know ID) can be prevented by this, and the outflow of data and the appearance of an inaccurate product can be avoided.

[0028] The key information written in a system area together on the other hand is used in order to encipher the raw data written in a data area in a user phase. That is, after reading a cryptographic key with the application which records data and changing raw data into encryption data using this cryptographic key, that encryption data is written in the data area of CD-R1. Also in case this cryptographic key decodes encryption data, it is used. That is, the input of ID is required with the application which reproduces data at the time of playback of data, coincidence with inputted ID and ID currently written in the system area is judged, in coincidence, a cryptographic key and encryption data are read, encryption data are decoded using the cryptographic key, it changes into raw data, and use of a user is presented.

[0029] Therefore, the inaccurate user who does not know ID Since the access to data itself is refused, while reading of inaccurate data is avoidable In the usual technical knowledge, even if access is successful with a certain means, since access to the cryptographic key written in the system area is impossible, it should not decode encryption data to raw data, but should devise a thoroughgoing security step in this point.

[0030] Drawing 4 is instantiation structural drawing of the data format containing ID information written in a system area at the time of manufacture, and a cryptographic key. In this drawing, the first example (a) has the magnitude of 20 bytes by all that consisted of each information on 8 bytes of ID information, 8 bytes of DES (Data Encryption Standard: U.S. federal government standard code specification) cryptographic key, 2 bytes of manufacture year, 1 byte of manufacture moon, and 1 byte of manufacture date. Moreover, the second example (b) has the magnitude of 36 bytes by all that consisted of each information on 8 bytes of ID information, 24 bytes of Triple DES cryptographic key, 2 bytes of manufacture year, 1 byte of manufacture moon, and 1 byte of manufacture date.

[0031] It is decided by whether the dependability of a cryptographic key is thought as important chiefly, or storage capacity pressure of a system area is avoided whether to

adopt format [ which ]. In addition, the byte count of illustration, the class of cryptographic key, and format structure are instantiation to the last. What is necessary is just to, write the information (ID information) in which solid-state discernment of CD-R1 is possible, and the key information on predetermined [ which can both be decoded from encryption data to raw data ] (cryptographic key) which can change raw data into encryption data in the system area of CD-R1 in short at the time of manufacture.

[0032] Drawing 5 is the rough block block diagram of a write-once mold optical disk record regenerative apparatus (henceforth a "CD-R record regenerative apparatus"). The spindle motor 12 which this CD-R record regenerative apparatus 10 supports the clamping area (information non-recording area prepared among T1-T2 of drawing 1 (a)) of CD-R1, and carries out a rotation drive in the predetermined direction, The optical pickup 14 which spaces substrate 1b of CD-R1, and irradiates the object for record, or the laser 13 for playback (generally infrared laser with a wavelength of 770-830nm) at recording layer 1c, While having the coarse adjustment motor 15 made to move an optical pickup 14 to radial [ of a disk ] in harmony with the seeking motor which is not illustrated [ which was prepared in the interior of an optical pickup 14 ] The disk roll control section 16 which controls the rotational speed of a spindle motor 12, The rotational speed of the coarse adjustment motor 15, and the coarse adjustment motor control section 17 which controls a hand of cut, The pickup control section 18 which performs control of the location of an optical pickup 14, or laser reinforcement, It has playback/record control section 19 which controls the reading signal from an optical pickup 14, conversion of waveform of the write-in signal to an optical pickup 14, etc., and has further the controller 20 which generalizes each of these control sections. This controller 20 is equivalent to an access means, an authentication means, and a permissible means given in the summary of invention.

[0033] the CD-R record regenerative apparatus 10 is built in the expansion slot of the host equipments 21, such as a personal computer, (or it carries out external -- having), connects between host equipment 21 and controllers 20 by cable 21a of predetermined signal specification (for example, SCSI:Small Computer System Interface), and is used.

[0034] The CD-R record regenerative apparatus 10 which has such a configuration can perform record and playback of recording information of the information on CD-R1 as it is shown below. in addition, CD-R1 -- CD-ROM -- although it is a compatible device and information playback of CD-ROM is also possible for the CD-R record regenerative apparatus 10, since there is no direct relation, explanation is

abbreviated to this invention.

[0035] If the application program only for CD-R records (it abbreviates to "AP" below.) is executed with <record actuation of information on CD-R1> host equipment 21, the laser on-the-strength calibration command from AP will be first told to a controller 20. While a controller 20 answers this command, tells a necessary command to each control section and locating an optical pickup 14 in an PCA sky field (field which is not tried, written and carried out) of CD-R1 After controlling rotational speed of a spindle motor 12 (it controls so that the relative velocity in the current position of an optical pickup 14 turns into a predetermined rate), the laser 13 for record of provisional reinforcement (arbitration power between 5.5-8mW) is irradiated from an optical pickup 14 to an PCA sky field, and trial writing is performed.

[0036] Subsequently, a controller 20 reads the data written [ were tried and ] and set to PCA through the playback record control section 19, and returns the data to AP of host equipment 21. AP tries and writes, compares data with expected value, judges the propriety of laser reinforcement, and if a judgment result is "**" while carrying out increase and decrease of the laser reinforcement of accommodation and publishing a laser on-the-strength calibration command again, if a judgment result is "no", it will start record actuation of the information on CD-R1.

[0037] This record actuation transmitting the necessary record data chosen suitably to a controller 20 from AP, and performing the roll control of a spindle motor 12, and position control of an optical pickup 14 through each control section under control of this controller 20 by the user, while modulating the laser 13 for record from an optical pickup 14 by the above-mentioned record data, it records on the data area of CD-R1. And if record is completed, while closing all sessions and writing TOC of the session information in a lead-in groove (RI), lead-out (RO) is formed after the last session.

[0038] In case the recording information of <playback actuation of recording information of CD-R1> CD-R1 is reproduced, Above AP (application program only for CD-R records) is unnecessary. However, the driver software for performing the interconversion of the file system of CD-R1 and the file system of host equipment 21 is indispensable. By using the CD-R record regenerative apparatus 10 through this driver software, a user can access the file system of CD-R1, without being conscious of distinction with other storage devices, such as a hard disk with which host equipment 21 was equipped. That is, since the file structure recognized by the file system of an operating system is in sight of a user, a user can choose the file stored in other storage devices, and the file made into the purpose in CD-R1 in the same procedure, the file is copied, it can stick on other storage devices, or, in the case of

execution files, such as an EXE format, the file concerned can be opened and performed.

[0039] While the CD-R record regenerative apparatus 10 reads the TOC information in a lead-in groove (RI) and provides the driver software of host equipment 21 with it on the occasion of this file access When the read-out command of a specific file is received from the driver software concerned While specifying the truck of a data area (UA) with which the data of the file concerned were written in with reference to the TOC information in a lead-in groove (RI) and locating an optical pickup 14 in the starting position of the truck Control the rotational speed of a spindle motor 12, irradiate the laser 13 for playback (the point that power is stopped by about 0.2mW is removed, and it is the same as the laser for record) from an optical pickup 14 at CD-R1, and the file data concerned is read. A series of actuation of transmitting the reading data to host equipment 21 is performed.

[0040] While the CD-R record regenerative apparatus 10 of the gestalt of this operation can write in information on CD-R1 as above, playback of the information written in CD-R1 can also be performed. Although this CD-R record regenerative apparatus 10 is an indispensable component when writing in information on CD-R1 in a user phase, it is a user phase and is a component needed also when reproducing information written in CD-R1. CD-R1 -- CD-ROM -- it is a compatible device, the CD-ROM regenerative apparatus is carried in most, such as a personal computer of these days, it is possible to perform information playback of CD-R1 using that CD-ROM regenerative apparatus, and since this CD-ROM regenerative apparatus cannot be accessed at ID information or the cryptographic key which were beforehand written in the system area of CD-R1, also when reproducing too information written in CD-R1, the CD-R record regenerative apparatus 10 is an indispensable component.

[0041] Moreover, although the CD-R record regenerative apparatus 10 is equipment chiefly used in a user phase, if it takes notice of the information write-in function to CD-R1, since it is applicable also to the writing of ID information or a cryptographic key performed in the manufacture phase of CD-R1, the fundamental actuation will go ahead with the talk by the following explanation as what is used in both a user phase and a manufacture phase in the above-mentioned CD-R record regenerative apparatus 10.

[0042] Information record processing > drawing 6 is a flow chart which shows the write-in actuation of ID information and a cryptographic key at the time of manufacture of CD-R1 (it says below, "it is information record processing at the time of shipment".) at the time of < shipment. In addition, in order to use only the record

function of the CD-R record regenerative apparatus 10 at the time of manufacture, in the flow chart of illustration, the thing of the CD-R record regenerative apparatus 10 is called the "record machine" for short for convenience. However, not only the CD-R record regenerative apparatus 10 but the intention of the purport which may be the "record machine" only for manufacture phases is included in this vocabulary (record machine).

[0043] In drawing, if information record processing is started at the time of shipment, first, non-recorded CD-R1 (a "disk" is called in a flow.) will be prepared, and a record machine will be loaded with this CD-R1 (step S11). next, host equipment 21 -- operating it -- the recording information to CD-R1 -- a manual entry -- or it generates automatically (step S12). This recording information is ID information on CD-R1, a predetermined private key, a date (creation data) on the day, etc., and that format is as being shown in drawing 4 (a) or (b).

[0044] Subsequently, if an information record instruction is published from host equipment 21 to a record machine (step S13), after a record machine answers this instruction, performs laser on-the-strength calibration processing and sets the laser 13 for record as proper power, it will carry out migration control of the optical pickup 14 in "the specific location" of the record section of CD-R1 (step S14). This specific location is an arbitration location on the field where direct access from a user is not accepted theoretically, i.e., the free space of a system area (PCA, PMA, a lead-in groove, or lead-out). It is an arbitration location (on a free space) on PCA currently especially recognized widely by this contractor preferably as a field where the existence is disregarded at the time of data playback, or PMA. Hereafter, let the above "a specific location" on [ of explanation ] expedient be an arbitration location on the free space of PCA.

[0045] Subsequently, modulating the laser 13 for record for recording information (information generated at step S12) using reception and its recording information from host equipment 21, it irradiates the laser 13 for record through transparent substrate 1b of CD-R1 at 1f of guide rails of recording layer 1c, forms an information pit in recording layer 1c of a guide rail 1f directly under, and a record machine performs the writing to CD-R1 of said recording information (step S15). The write-in starting position of recording information is the migration location of the optical pickup 14 performed at the above-mentioned step S14, i.e., the arbitration location on the free space of PCA, and the write-in termination location of recording information is a location which separated only the part equivalent to the size (it will be 20 bytes or 36 bytes if a format of drawing 4 is followed) of recording information from the location

concerned.

[0046] Subsequently, a record machine reproduces recording information written in the system area by making into a playback termination location the location from which only the part equivalent to a playback starting position and the size of recording information separated the location concerned, and transmits this playback information to host equipment 21 while it moves an optical pickup 14 to the above-mentioned specific location, i.e., the arbitration location on the free space of PCA. While judging that host equipment 21 was able to be normally written in when comparison collating of the playback data and the above-mentioned recording information which were transmitted from the record machine was carried out, verification inspection was conducted (step S16) and both were in agreement and reporting that to an operator, it judges that writing went wrong and that is reported to an operator (step S17). In normal write-in information, an operator moves CD-R1 concerned to a shipment shelf (step S18), and, in write-in failure information, moves CD-R1 concerned to a defective shelf (step S19). And the above processing is repeatedly performed until prepared CD-R1 is lost (step S20).

[0047] Therefore, according to this "being information record processing at the time of shipment", hiding information, such as ID information, a cryptographic key, and creation data, can be written in the system area of non-recorded CD-R1, and it can ship to a commercial scene, and can send to a user. And in case data write-in processing, data regeneration, or disk copy processing in which it explains below is performed in a user phase, processing peculiar to the gestalt of this operation using the above-mentioned hiding information can be performed.

[0048] <Data write-in processing by user> drawing 7 is a flow chart which shows the data write-in actuation (henceforth "data write-in processing by the user") performed in a user phase. In this processing, a user receives CD-R1 in which it hid by information record processing at the time of the above-mentioned shipment, and information was written in a commercial scene, sets that CD-R1 in the CD-R record regenerative apparatus 10, and records necessary user data on CD-R1 concerned. About this user data, an especially important point is in the point which is the secret data which permit playback only to a specific man, i.e., the data which require secrecy. When the data which require this kind of secrecy were conventionally recorded on CD-R, data were enciphered by the predetermined cryptographic key, it recorded on CD-R, and storages, such as a floppy disk which stored the decode key of the encryption data concerned together with that CD-R, were distributed. However, coincidence distribution of such multimedia has possibility, such as loss at a

distribution place, when taking time and effort, and it has the fault that management is troublesome.

[0049] CD-R1 of the gestalt of this operation has the merit that management is made easy and it can cancel above-mentioned un-arranging, without losing at a distribution place, since encryption data and the decode key of the encryption data are stored and distributed to one storage.

[0050] In drawing 7 , if the data write-in processing by the user is started, the CD-R record regenerative apparatus 10 will judge the existence of the write-in instruction from host equipment 21 (step S31). And if there is a write-in instruction, ID input request is published to host equipment 21 (step S32), and ** will display predetermined GUI (Graphical User Interface) of **** for ID input on a screen, and host equipment 21 will receive ID input from the keyboard by the user etc. (step S33), and will transmit inputted ID information to the CD-R record regenerative apparatus 10.

[0051] If it is coincidence while the CD-R record regenerative apparatus 10 reads ID information currently written in the system area of CD-R1, judges coincidence with ID information transmitted from host equipment 21 (step S34), and it will end processing as it is, if it is inharmonious, it will read the cryptographic key currently written in the system area of CD-R1, and will transmit it to host equipment 21 (step S35). Host equipment 21 changes the above-mentioned user data into encryption data using the cryptographic key (step S36), and transmits the encryption data concerned to the CD-R record regenerative apparatus 10. The CD-R record regenerative apparatus 10 ends processing, after recording the transmitted encryption data on the data area of CD-R1 (step S37).

[0052] Drawing 8 is drawing showing the time run of the above "data write-in processing by the user", and the thing equivalent to the host equipment 21 above-mentioned [ the personal computer 31 in drawing ], the thing equivalent to the CD-R record regenerative apparatus 10 above-mentioned [ the CD-R writer 32 ], and CD-R33 are equivalent to above-mentioned CD-R1.

[0053] In this drawing, while a user loads the CD-R writer 32 with CD-R33, he operates a personal computer 31 and publishes a necessary write-in instruction for the CD-R writer 32. The CD-R writer 32 answers this write-in instruction, ID request is returned to a personal computer 31, and, as for a personal computer 31, ** displays GUI of **** for ID input on a screen. A user inputs predetermined ID information (ID information told by the salesman etc. at the time of the purchase of CD-R33) according to the GUI, and a personal computer 31 transmits inputted ID information to

the CD-R writer 32.

[0054] ID information currently beforehand written in the system area of CD-R33 will be read, the CD-R writer 32 judges coincidence with ID information transmitted from the personal computer 31, if in agreement while stopping processing and refusing writing, if inharmonious, will read the cryptographic key currently beforehand written in the system area of CD-R33, and will transmit it to a personal computer 31. A personal computer 31 enciphers user data using the cryptographic key, and transmits encryption data to the CD-R writer 32. After the CD-R writer 32 records encryption data on the data area of CD-R33, it notifies completion of record actuation to a personal computer 31, and ends "data write-in processing by the user" of an above single string.

[0055] Therefore, while being able to perform user authentication using ID information beforehand written in the system area of CD-R according to this "processing data write-in [ by the user ]", in the case of the data writing performed by the authentication user (registered user), a user data encryption can be performed using the cryptographic key beforehand written in the system area of CD-R, and that encryption data can be written in CD-R.

[0056] Consequently, that what is necessary is just to operate and write in host equipment and to perform assignment of the target user data, and the input of ID information, a user can automate the writing to CD-R of the user data encryption processing concerned and encryption data, and can aim at an improvement of workability.

[0057] <Data regeneration by user> drawing 9 is a flow chart which shows the data playback actuation (henceforth "data regeneration by the user") performed in a user phase. In this processing, a user receives CD-R1 in which encryption data were written by the data write-in processing by the above-mentioned user, sets that CD-R1 in the CD-R record regenerative apparatus 10, reads a cryptographic key and encryption data from that CD-R1, and performs a series of processings in which encryption data are decoded using a cryptographic key. An especially important point is in this the processing of a series of for two kinds of users to exist. The first user is a user (henceforth a "registered user") who knows just ID information, and the second user is a user (henceforth an "inaccurate user") who does not know just ID information.

[0058] In drawing 9 , if the data regeneration by the user is started, the CD-R record regenerative apparatus 10 will judge the existence of the playback instruction from host equipment 21 (step S41). And if there is a playback instruction, ID input request

is published to host equipment 21 (step S42), and ** will display predetermined GUI of **** for ID input on a screen, and host equipment 21 will receive ID input from the keyboard by the user etc. (step S43), and will transmit inputted ID information to the CD-R record regenerative apparatus 10.

[0059] The CD-R record regenerative apparatus 10 reads ID information currently written in the system area of CD-R1. Judge coincidence with ID information transmitted from host equipment 21 (step S44), and if inharmonious, while judging it as an inaccurate user and ending processing as it is, if it is coincidence, it will be judged as a registered user. The cryptographic key currently written in the system area of CD-R1 and the encryption data currently written in the data area are read, and it transmits to host equipment 21 (step S45). After host equipment 21 decodes encryption data using the cryptographic key and permits a registered user's access to the decode data concerned, it ends processing.

[0060] Drawing 10 is drawing showing the time run of the above "data regeneration by the user", and the thing equivalent to the host equipment 21 above-mentioned [ the personal computer 31 in drawing ], the thing equivalent to the CD-R record regenerative apparatus 10 above-mentioned [ the CD-R writer 32 ], and CD-R33 are equivalent to above-mentioned CD-R1.

[0061] In this drawing, while a user loads the CD-R writer 32 with CD-R33, he operates a personal computer 31 and publishes a necessary playback instruction for the CD-R writer 32. The CD-R writer 32 answers this playback instruction, ID request is returned to a personal computer 31, and, as for a personal computer 31, ** displays GUI of **** for ID input on a screen. A user inputs predetermined ID information (ID information justly notified from the distribution place of CD-R33) according to the GUI, and a personal computer 31 transmits inputted ID information to the CD-R writer 32.

[0062] The CD-R writer 32 reads ID information currently beforehand written in the system area of CD-R33, and coincidence with ID information transmitted from the personal computer 31 is judged. If inharmonious, while judging it as an inaccurate user, stopping processing and refusing playback If in agreement, it will be judged as a registered user, and the cryptographic key currently beforehand written in the system area of CD-R33 and the encryption data currently written in the data area are read, and it transmits to a personal computer 31. After a personal computer 31 decodes encryption data using the cryptographic key and permits access from a registered user, it ends "data regeneration by the user" of an above single string.

[0063] Therefore, while a registered user and an inaccurate user are discriminable using ID information beforehand written in the system area of CD-R according to this

"data regeneration by the user" Restrict, when data regeneration is performed by the registered user, and the cryptographic key written in the system area of CD-R and the encryption data written in the data area are transmitted to host equipment. Encryption data can be decoded with host equipment and accesses (for example, perusal thru/or activation, etc. of data) to the decoded raw data can be permitted.

[0064] consequently, an inaccurate user -- eliminating -- playback of data -- it can carry out -- unjust perusal, unjust activation, etc. of data -- preventing -- with -- **** -- the security nature of CD-R can be improved.

[0065] <Disk copy processing by user> drawing 11 is a flow chart which shows the disk copy actuation (henceforth "disk copy processing by the user") performed in a user phase. In this processing, by data write-in processing by the above-mentioned user, a user receives CD-R1 in which encryption data were written, and sets that CD-R1 in the CD-R record regenerative apparatus 10. A cryptographic key and encryption data are read from the CD-R1, encryption data are decoded using the cryptographic key concerned, and a series of processings in which the decode data is written in intact CD-R set in another CD-R record regenerative apparatus 10 (it copies) are performed. Also in this the processing of a series of, two kinds of users of the inaccurate user who does not know just ID information with the registered user who knows just ID information exist.

[0066] In drawing 11 , if the disk copy processing by the user is started, the CD-R record regenerative apparatus (henceforth a "copied material CD-R record regenerative apparatus") 10 loaded with CD-R1 of a copied material will judge the existence of the copy instruction from host equipment 21 (step S51). And if there is a copy instruction, ID input request is published to host equipment 21 (step S52), and ** will display predetermined GUI of **** for ID input on a screen, and host equipment 21 will receive ID input from the keyboard by the user etc. (step S53), and will transmit inputted ID information to the copied material CD-R record regenerative apparatus 10.

[0067] The copied material CD-R record regenerative apparatus 10 reads ID information currently written in the system area of CD-R1. Coincidence with ID information transmitted from host equipment 21 is judged (step S54). If inharmonious, while reading the encryption data which judged it as the inaccurate user and were written in the data area of CD-R1 and transmitting to host equipment 21 (step S55) If it is coincidence, the encryption data currently written in ID information, cryptographic key, and data area which judge it as a registered user and are written in the system area of CD-R1 will be read, and it will transmit to host equipment 21 (step S56).

[0068] Host equipment 21 judges whether ID information and a cryptographic key are contained in the transfer data. If ID information and a cryptographic key are contained, it is the CD-R record regenerative apparatus 10 (it is called below a "copy place CD-R record regenerative apparatus".) of a copy place one by one about the ID information and cryptographic key, and encryption data. It transmits to 10, or if ID information and a cryptographic key are not contained, transfer data (encryption data) itself is transmitted to the copy place CD-R record regenerative apparatus 10.

[0069] The copy place CD-R record regenerative apparatus 10 is the same procedure as above-mentioned "being information record processing at the time of shipment" (referring to drawing 6 ), when ID information and key information are included in the transmitted data. After recording the ID information and key information on CD-R of a copy place, encryption data are recorded on the data area of CD-R of a copy place. Or when ID information and key information are not included in the transmitted data, after recording encryption data on the data area of CD-R of a copy place, the completion of record is notified to host equipment 21, and a series of disk copy processings are ended.

[0070] Drawing 12 is drawing showing the time run of the above "disk copy processing by the user." The thing equivalent to the host equipment 21 above-mentioned [ the personal computer 31 in drawing ], That by which left-hand side CD-R33a is equivalent to CD-R1 of a copied material, the thing by which left-hand side CD-R writer 32a is equivalent to the above-mentioned copied material CD-R record regenerative apparatus 10, CD-R33b of the thing and right-hand side on which right-hand side CD-R writer 32b is equivalent to the above-mentioned copy place CD-R record regenerative apparatus 10 is equivalent to CD-R of a copy place. That is, this example shows the example which carries out the disk copy of the recording information of left-hand side CD-R33a to right-hand side CD-R33b.

[0071] In this drawing, while a user loads the CD-R writers 32a and 32b with CD-Rs 33a and 33b of a copy place a copied material, respectively, he operates a personal computer 31 and publishes a necessary copy instruction to copied material CD-R writer 32a. Copied material CD-R writer 32a answers this copy instruction, and returns ID request to a personal computer 31, and, as for a personal computer 31, ** displays GUI of **** for ID input on a screen. A user inputs predetermined ID information (ID information justly notified from the distribution place of CD-R33a) according to the GUI, and a personal computer 31 transmits inputted ID information to copied material CD-R writer 32a.

[0072] Copied material CD-R writer 32a reads ID information currently beforehand

written in the system area of CD-R33a, and coincidence with ID information transmitted from the personal computer 31 is judged. If inharmonious, while it is judged as an inaccurate user and the restrictive copy of only encryption data is permitted If in agreement, it will be judged as a registered user, and the encryption data currently written in ID information, cryptographic key, and data area which are beforehand written in the system area of CD-R33a are read, and it transmits to a personal computer 31.

[0073] A personal computer 31 transmits ID information, the cryptographic key, and encryption data which were read from CD-R33a of a copied material to copy place CD-R writer 32b while publishing a write-in instruction to copy place CD-R writer 32b. Copy place CD-R writer 32b writes the encryption data in the data area of CD-R33b, notifies the write-in completion to host equipment 21, and ends "disk copy processing by the user" of an above single string while it writes the ID information and cryptographic key in the system area of CD-R33b.

[0074] Therefore, while a registered user and an inaccurate user are discriminable using ID information beforehand written in the system area of copied material CD-R according to this "disk copy processing by the user" It restricts, when disk copy processing is performed by the registered user. The encryption data written in ID information, cryptographic key, and data area which were written in the system area of copied material CD-R can be transmitted to host equipment, and it can transmit to a copy place CD-R writer from host equipment, and can write in copy place CD-R (it copies).

[0075] Consequently, while a disk copy can be permitted only to a registered user and the perfect by-product of copied material CD-R can be made to manufacture, the restrictive copy of only encryption data can be permitted to an inaccurate user, the incomplete by-product (data cannot be used unless a code is decoded) which is not reusable can be made to be able to manufacture substantially, the appearance of unjust duplicate objects, such as a pirate edition CD, can be prevented, and improvement in the security nature of CD-R can be aimed at.

[0076] As explained more than the <conclusion> CD-R1 of the gestalt of this operation Since ID information and the hiding information of a cryptographic key are written in and shipped to the specific field (system area) to which direct access by the user is not accepted By mounting the security function which used the hiding information for the CD-R writer (CD-R record regenerative apparatus 10) used in the case of the data writing of a user phase, or data playback It becomes possible to attest the access permission to CD-R1, and data writing and data playback can be

permitted only to a registered user.

[0077] therefore, the description (elimination and an alteration of data are impossible) of a write-once mold -- in addition, a commercial scene can be provided with CD-R1 which gave still more positive security nature, and the social benefit that it applies to the storage of data and the field of distribution which require especially secrecy, and a very desirable write-once mold optical disk can be realized can be done so.

[0078] in addition, in the above explanation, although hiding information, such as ID information and a cryptographic key, is written in the system area, this system area may be the semantics of fields other than the field (typically data area) where direct access by the user was permitted, and you may be a lead-in groove not to mention above-mentioned PCA and PMA, and may be lead-out, or fields other than this exist -- you may be that field as long as it becomes.

[0079] Moreover, although explanation was not added especially about a cryptographic key, any of various cipher systems (for example, there are methods, such as FEAL:Fast Encipherment Algorithm, besides the above-mentioned DES method.) which are generally known may be adopted. What is necessary is to take into consideration the difficulty of decode, the overhead of encryption processing or decode processing, the volume of encryption data, etc., and just to adopt a suitable method.

[0080] Moreover, the security function using ID information and the cryptographic key of said explanation The hardware property containing the microcomputer and the various peripheral devices which were chiefly mounted in the controller 20 of the CD-R record regenerative apparatus 10, or the main board of host equipment 21, Although organic association with software property, such as an operating system and various programs (driver software is included), realizes functionally Since hardware property and an operating system can use a general-purpose thing The indispensable matter indispensable for a security function in which ID information and the cryptographic key of said explanation were used Substantially, being together put by programs, such as the above-mentioned "data write-in processing by the user" (referring to drawing 7 ), "data regeneration by the user" (referring to drawing 9 ), and "disk copy processing by the user" (referring to drawing 11 ), can say.

[0081] Therefore, the security function using ID information concerning this invention or a cryptographic key includes the component (a unit article, a finished product, or semifinished product) containing record media or these record media, such as the floppy disk and optical disk which stored all those programs or its important section, a compact disk, a magnetic tape, a hard disk, or semiconductor memory. In addition,

what the record medium or component has on a network not to mention that by which itself is in a distribution channel, and offers only the contents of record is contained.

[0082] Moreover, in the above explanation, although the example of CD-R was shown as a write-once mold optical disk, it does not restrict to this. For example, since DVD(Digital Video Disc or Digital Versatile Disc)-R can also perform one data writing, of course, he is the associate of a write-once mold optical disk. What is necessary is to read a CD-R record regenerative apparatus and a CD-R writer with a DVD-R record regenerative apparatus and a DVD-R writer, respectively, and just to replace them, while reading CD-R as DVD-R, when applying the above-mentioned explanation to DVD-R.

[0083]

[Effect of the Invention] Since according to invention according to claim 1 the information for the security countermeasures written in the system area maintains the invisible condition from a user and is shipped, the information concerned can be made into the hiding information from a user.

[0084] According to invention according to claim 2, the information for security countermeasures is written in and shipped to the specific field (field for laser on-the-strength calibrations) to which the existence is disregarded at the time of playback of data. Since the field concerned is widely understood as an object for laser on-the-strength calibrations also for about [ that it is invisible ] and this contractor to the user, it can secure invisibility also to this contractor that has this know how.

[0085] According to invention according to claim 3, the information for security countermeasures is written in the field to which direct access from a user is not permitted, and all are shipped to it. Therefore, the information concerned can be made into the hiding information from a user.

[0086] According to invention according to claim 4, the user authentication using the information for security countermeasures becomes possible in a user phase. Therefore, an inaccurate user can be eliminated using this authentication result, and record of data and the security at the time of playback can be improved.

[0087] According to invention according to claim 5, the user data encryption using the information for security countermeasures becomes possible in a user phase. Therefore, since it is not exposed of raw data even when unjust authentication should be carried out, the secrecy nature of data is securable.

[0088] According to invention according to claim 6, the decode using the information for security countermeasures of encryption data is attained in a user phase. Therefore, even when unjust authentication should be carried out, unless the

information for security countermeasures is read, it cannot be exposed of raw data and the secrecy nature of data can be secured.

[0089] According to invention according to claim 7, by loading with the write-once mold optical disk with which the information for security countermeasures was written in a part of system area, and using the information for the security countermeasures, authentication processing of a registered user is attained, for example, data logging to said write-once mold optical disk and the security in the case of the data playback from said write-once mold optical disk can be secured. therefore, the description (elimination and an alteration of data are impossible) of a write-once mold optical disk -- in addition, a more positive data integrity measure can be taken, it uses for the storage of data and the field of distribution which require especially secrecy, and the suitable record regenerative apparatus for write-once mold optical disks can be offered.

[0090] According to invention according to claim 8, said access means, an authentication means, and a permissible means are realizable with organic association with the hardware property and this program containing a microcomputer.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1] It is the external view and its important section enlarged drawing of a write-once mold optical disk.

[Drawing 2] It is cross-section structural drawing of CD-R.

[Drawing 3] It is the format conceptual diagram of each record section of CD-R.

[Drawing 4] It is instantiation structural drawing of the data format containing ID information written in a system area at the time of manufacture, and a cryptographic key.

[Drawing 5] It is the rough block block diagram of a write-once mold optical disk record regenerative apparatus.

[Drawing 6] It is the flow chart which shows the write-in actuation of ID information and a cryptographic key at the time of manufacture of CD-R (at the time of shipment information record processing).

[Drawing 7] It is the flow chart which shows the data write-in actuation (data write-in processing by the user) performed in a user phase.

[Drawing 8] It is drawing showing the time run of the data write-in processing by the user.

[Drawing 9] It is the flow chart which shows the data playback actuation (data regeneration by the user) performed in a user phase.

[Drawing 10] It is drawing showing the time run of the data regeneration by the user.

[Drawing 11] It is the flow chart which shows the disk copy actuation (disk copy processing by the user) performed in a user phase.

[Drawing 12] It is drawing showing the time run of the disk copy processing by the user.

[Description of Notations]

PCA Power Calibration Area (a system area, field for laser on-the-strength calibrations)

PMA Program Memory Area (a system area, field for temporary storages of session information)

RI Lead-in groove (field for session information storing)

RO Lead-out (field for specifying the termination location of a user area)

UA User area (user area)

1 CD-R (Write-once Mold Optical Disk)

10 CD-R Record Regenerative Apparatus (Record Regenerative Apparatus for Write-once Mold Optical Disks)

20 Controller (Access Means, Authentication Means, Permissible Means)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－319339
（P2001－319339A）
(43)公開日　平成13年11月16日(2001.11.16)

| (51)Int.Cl.⁷ | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｇ１１Ｂ　7/005 | | Ｇ１１Ｂ　7/005 | Ｚ | ５Ｂ０１７ |
| Ｇ０６Ｆ　12/14 | ３２０ | Ｇ０６Ｆ　12/14 | ３２０Ａ | ５Ｄ０４４ |
| Ｇ１１Ｂ　19/02 | ５０１ | Ｇ１１Ｂ　19/02 | ５０１Ｊ | ５Ｄ０６６ |
| 20/10 | | 20/10 | Ｈ | ５Ｄ０９０ |

審査請求　未請求　請求項の数８　ＯＬ　（全 16 頁）

(21)出願番号　特願2000－138346(P2000－138346)

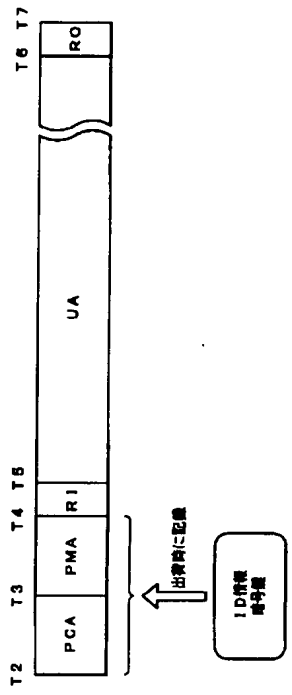
(22)出願日　平成12年５月11日(2000.5.11)

(71)出願人　000204284
太陽誘電株式会社
東京都台東区上野６丁目16番20号
(72)発明者　大村　幸秀
東京都台東区上野６丁目16番20号　太陽誘電株式会社内
(72)発明者　砂川　隆一
東京都台東区上野６丁目16番20号　太陽誘電株式会社内
(74)代理人　100096699
弁理士　鹿嶋　英實

最終頁に続く

(54)【発明の名称】　ライトワンス型光ディスク、ライトワンス型光ディスク用記録再生装置および記録媒体。

(57)【要約】
【課題】　ライトワンス型光ディスクの記録情報の不正読み出しを防止する。
【解決手段】　ユーザデータを書き込むためのユーザ領域と、少なくとも当該書き込み動作を行う際にシステムによって利用されるシステム領域とを備えたライトワンス型光ディスクにおいて、前記システム領域の一部にセキュリティ対策のための情報を書き込んで出荷する。システム領域に書き込まれたセキュリティ対策のための情報がユーザからの不可視状態を保って出荷されるため、当該情報をユーザからの隠し情報とすることができ、この隠し情報を利用することにより、記録情報の不正読み出しの防止が可能となる。



1

【特許請求の範囲】

【請求項１】　ユーザデータを書き込むためのユーザ領域と、少なくとも当該書き込み動作を行う際にシステムによって利用されるシステム領域とを備えたライトワンス型光ディスクにおいて、

前記システム領域の一部にセキュリティ対策のための情報を書き込んで出荷するようにしたことを特徴とするライトワンス型光ディスク。

【請求項２】　前記システム領域は、ユーザデータを書き込む際のレーザ強度キャリブレーション用領域であることを特徴とする請求項１記載のライトワンス型光ディスク。

【請求項３】　前記システム領域は、ユーザデータを書き込む際のセッション情報の一時格納用領域、または、ユーザ領域に書き込まれたユーザデータを再生する際に参照されるセッション情報格納用領域、若しくは、ユーザ領域の終了位置を明示するための領域のいずれかであることを特徴とする請求項１記載のライトワンス型光ディスク。

【請求項４】　前記セキュリティ対策のための情報は、ユーザ認証のための識別情報であることを特徴とする請求項１記載のライトワンス型光ディスク。

【請求項５】　前記セキュリティ対策のための情報は、前記ユーザデータを暗号化するための鍵情報であることを特徴とする請求項１記載のライトワンス型光ディスク。

【請求項６】　前記セキュリティ対策のための情報は、前記ユーザ領域に書き込まれた暗号化データを復号するするための鍵情報であることを特徴とする請求項１記載のライトワンス型光ディスク。

【請求項７】　システム領域の一部にセキュリティ対策のための情報が書き込まれたライトワンス型光ディスクにアクセスするアクセス手段と、

前記アクセス手段によって読み出された前記セキュリティ対策のための情報と外部から入力された認証情報との一致を判定してユーザ認証を行う認証手段と、

前記認証手段によって正規ユーザの認証が行われた場合に前記ライトワンス型光ディスクへの外部からのアクセスを許容する許容手段と、

を備えたことを特徴とするライトワンス型光ディスク用記録再生装置。

【請求項８】　システム領域の一部にセキュリティ対策のための情報が書き込まれたライトワンス型光ディスクにアクセスするアクセス手段と、

前記アクセス手段によって読み出された前記セキュリティ対策のための情報と外部から入力された認証情報との一致を判定してユーザ認証を行う認証手段と、

前記認証手段によって正規ユーザの認証が行われた場合に前記ライトワンス型光ディスクへの外部からのアクセスを許容する許容手段とを実現するためのプログラムを格納したことを特徴とする記録媒体。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ライトワンス型光ディスク、ライトワンス型光ディスク用記録再生装置および記録媒体に関する。詳しくは、１回だけデータを書き込むことができるＣＤ－Ｒ（Compact Disc Recordable）に代表されるライトワンス型光ディスク、ライトワンス型光ディスク用記録再生装置および記録媒体に関する。

【０００２】

【従来の技術】各種コンテンツやコンピュータプログラム等の電子データの配布媒体として、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）が多用されている。ＣＤ－ＲＯＭは、電子データを記録したマスタＣＤからプレス成型等によって製造された副生物であり、主に大量配布のメディアに用いられるが、配布数（製造数）の少ないサンプル版ＣＤやプライベートＣＤなどには、ライトワンス型の光ディスク装置、すなわちＣＤ－Ｒが用いられる。ＣＤ－Ｒは透明なディスク基板と反射層（詳細な構造は後述する。）との間に有機色素からなる記録層を有している点でＣＤ－ＲＯＭと構造上の相違があり、専用の記録装置（ＣＤ－Ｒライター）を用いて当該記録層に高出力レーザを照射し、熱的反応によって当該記録層に情報ピットを形成することにより、ユーザ段階で情報の記録を行うことができるものである。

【０００３】ＣＤ－Ｒは上記のとおり情報の消去や上書きができない（追記は可能）ライトワンス型である。すなわち、一度書き込んだ情報の消去や書き換えが不可能である。したがって、不正者による情報の消去や改ざんを確実に防止できるという優れた利点を持つことから、特に保全を要する電子データの配布や保管などの用途に欠かせない記憶媒体となっている。

【０００４】

【発明が解決しようとする課題】しかしながら、従来のライトワンス型光ディスクにあっては、記録情報の消去や改ざんを防止できるという優れた利点があるものの、記録情報の読み出しが自由であるため、記録情報の不正読み出しや不正コピーを防止できないという不都合があった。このため、秘匿を要する情報を記録したＣＤ－Ｒの保管に際しては、厳格な管理規則を適用しなければならないが、このような管理規則の運用は相当困難で、多くの場合、規則の不徹底や馴れなどから安易な傾向に流れやすく、不心得な者によるＣＤ－Ｒの持ち出しや情報の読み出しを阻止できない結果、秘匿すべき情報の外部流出ないしは不正にコピーされたＣＤ－Ｒの出現を回避できないという問題点があった。

【０００５】なお、かかる問題点は、ＣＤ－Ｒに限らず、可搬型の記憶デバイス一般にいえることであるが、ＣＤ－Ｒについては特に深刻である。ＣＤ－Ｒは、その

ライトワンス型の特徴を活かして保全を要する電子データの配布や保管などに広く用いられている現実に加え、不要になったＣＤ－Ｒを物理的に破壊（例えば、意図的に傷をつけたり切断したりする）しない限り、用済み後もその記録情報の不正読み取りが可能であるからである。

【０００６】したがって、本発明が解決しようとする課題は、ライトワンス型光ディスクの記録情報の不正読み出しを防止し、以って特に保全を要する電子データの配布や保管などの用途に適合するライトワンス型光ディスクを提供することにある。

【０００７】

【課題を解決するための手段】請求項１記載のライトワンス型光ディスクは、ユーザデータを書き込むためのユーザ領域と、少なくとも当該書き込み動作を行う際にシステムによって利用されるシステム領域とを備えたライトワンス型光ディスクにおいて、前記システム領域の一部にセキュリティ対策のための情報を書き込んで出荷するようにしたことを特徴とする。これによれば、システム領域に書き込まれたセキュリティ対策のための情報がユーザからの不可視状態を保って出荷される。

【０００８】請求項２記載のライトワンス型光ディスクは、請求項１記載のライトワンス型光ディスクにおいて、前記システム領域は、ユーザデータを書き込む際のレーザ強度キャリブレーション用領域であることを特徴とする。これによれば、データの再生時にその存在が無視される特定の領域（レーザ強度キャリブレーション用領域）にセキュリティ対策のための情報が書き込まれて出荷される。

【０００９】請求項３記載のライトワンス型光ディスクは、請求項１記載のライトワンス型光ディスクにおいて、前記システム領域は、ユーザデータを書き込む際のセッション情報の一時格納用領域、または、ユーザ領域に書き込まれたユーザデータを再生する際に参照されるセッション情報格納用領域、若しくは、ユーザ領域の終了位置を明示するための領域のいずれかであることを特徴とする。これによれば、いずれもユーザからの直接的なアクセスが許容されていない領域にセキュリティ対策のための情報が書き込まれて出荷される。

【００１０】請求項４記載のライトワンス型光ディスクは、請求項１記載のライトワンス型光ディスクにおいて、前記セキュリティ対策のための情報は、ユーザ認証のための識別情報であることを特徴とする。これによれば、ユーザ段階で、セキュリティ対策のための情報を利用したユーザ認証が可能となる。

【００１１】請求項５記載のライトワンス型光ディスクは、請求項１記載のライトワンス型光ディスクにおいて、前記セキュリティ対策のための情報は、前記ユーザデータを暗号化するための鍵情報であることを特徴とする。これによれば、ユーザ段階で、セキュリティ対策のための情報を利用したユーザデータの暗号化が可能となる。

【００１２】請求項６記載のライトワンス型光ディスクは、請求項１記載のライトワンス型光ディスクにおいて、前記セキュリティ対策のための情報は、前記ユーザ領域に書き込まれた暗号化データを復号するするための鍵情報であることを特徴とする。これによれば、ユーザ段階で、セキュリティ対策のための情報を利用した暗号化データの復号が可能となる。

【００１３】請求項７記載のライトワンス型光ディスク用記録再生装置は、システム領域の一部にセキュリティ対策のための情報が書き込まれたライトワンス型光ディスクにアクセスするアクセス手段と、前記アクセス手段によって読み出された前記セキュリティ対策のための情報と外部から入力された認証情報との一致を判定してユーザ認証を行う認証手段と、前記認証手段によって正規ユーザの認証が行われた場合に前記ライトワンス型光ディスクへの外部からのアクセスを許容する許容手段と、を備えたことを特徴とする。これによれば、システム領域の一部にセキュリティ対策のための情報が書き込まれたライトワンス型光ディスクを装填して、そのセキュリティ対策のための情報を利用することにより、正規ユーザの認証処理が可能となり、例えば、前記ライトワンス型光ディスクへのデータ記録や、前記ライトワンス型光ディスクからのデータ再生の際のセキュリティが確保される。

【００１４】請求項８記載の記録媒体は、システム領域の一部にセキュリティ対策のための情報が書き込まれたライトワンス型光ディスクにアクセスするアクセス手段と、前記アクセス手段によって読み出された前記セキュリティ対策のための情報と外部から入力された認証情報との一致を判定してユーザ認証を行う認証手段と、前記認証手段によって正規ユーザの認証が行われた場合に前記ライトワンス型光ディスクへの外部からのアクセスを許容する許容手段とを実現するためのプログラムを格納したことを特徴とする。これによれば、マイクロコンピュータを含むハードウェア資産と該プログラムとの有機的結合によって前記アクセス手段、認証手段および許容手段が実現される。

【００１５】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を詳細に説明する。なお、以下の説明における様々な細部の特定ないし実例および数値や文字列その他の記号の例示は、本発明の思想を明瞭にするための、あくまでも参考であって、それらのすべてまたは一部によって本発明の思想が限定されないことは明らかである。また、周知の手法、周知の手順、周知のアーキテクチャおよび周知の回路構成等（以下「周知事項」）についてはその細部にわたる説明を避けるが、これも説明を簡潔にするためであって、これら周知事項のすべてまたは一

部を意図的に排除するものではない。かかる周知事項は本発明の出願時点で当業者の知り得るところであるので、以下の説明に当然含まれている。

【００１６】図１は、ライトワンス型光ディスク（以下「ＣＤ－Ｒ」という。）の外観図（ａ）およびその要部拡大図（ｂ）である。これらの図において、ＣＤ－Ｒ１は、直径１２ｃｍ（直径８ｃｍのものもある。以下、直径１２ｃｍのもので説明する。）のディスク状を有しており、ディスクの中心に直径１５ｍｍのセンターホール１ａが形成されている。ディスクの中心Ｔ０からセンターホール１ａの壁（ディスク内縁Ｔ１）までの距離は７．５ｍｍ、Ｔ０からディスク外縁Ｔ７までの距離は６０ｍｍであり、このＴ１～Ｔ７の間に同心状の複数の記録領域、すなわち、ディスクの内周側から順にＰＣＡ（Power Calibration Area）、ＰＭＡ（Program Memory Area）、リードイン（図では「ＲＩ」と略している。）、データエリア（図では「ＵＡ」と略している。）およびリードアウト（図では「ＲＯ」と略している。）の各領域が設けられている。

【００１７】各領域を概説すると、Ｔ２～Ｔ３に位置するＰＣＡは、ＣＤ－Ｒ１にデータを記録する際に行われるレーザ強度調整のための試し書き領域である。この試し書きは一般に１００回程度可能であり、少なくとも１回のデータ記録で１回分の領域を消費する。Ｔ３～Ｔ４に位置するＰＭＡは、ＣＤ－Ｒ１でまだクローズしていないセッションのトラックがあるとき、そのトラック番号と開始／終了位置を一時的に保存する領域である。Ｔ４～Ｔ５に位置するリードイン（ＲＩ）は、セッショントラックの先頭（ディスクの内周側）にある領域で、セッションのＴＯＣ（Table Of Contents：ＣＤに記録されているトラック数、開始位置およびデータ領域の合計の長さ）を保存する領域である。セッションをクローズすると、ＰＭＡに一時保存されていた情報がこのリードイン（ＲＩ）に書き込まれる。

【００１８】Ｔ５～Ｔ６に位置するデータエリア（ＵＡ）は、ユーザ段階で実際にデータが書き込まれる領域である。データの記録容量は最大約６８０Ｍバイト（直径８ｃｍのものは最大約１９０Ｍバイト）であり、この記憶容量は録音時間で表すと最大約７４分（直径８ｃｍのものは最大約２１分）になる。データエリア（ＵＡ）は、リードイン（ＲＩ）のすぐ後ろから連続する所定サイズ（２Ｋバイト）単位の論理ブロックで管理されるようになっており、各論理ブロックごとに０から最大約３３０００までのＬＢＮ（Logical Block Number）が割り当てられるようになっている。Ｔ６～Ｔ７に位置するリードアウト（ＲＯ）は、セッションの最後（ディスクの外周側）にある領域で、データエリア（ＵＡ）の最後に到達したことを示す領域である。

【００１９】これら各領域のディスク上の位置はＴ２とＴ３を除いて規格化されている。すなわち、Ｔ４はＴ０から２３ｍｍ離れた位置、Ｔ５はＴ０から２５ｍｍ離れた位置、Ｔ６はＴ０から５８ｍｍ離れた位置となるように規定されている。なお、図ではディスク外縁とリードアウト（ＲＯ）の終了位置とを同一の符号（Ｔ７）で示しているが、これは図示の都合である。リードアウト（ＲＯ）の実際の終了位置はＴ０から５８．５ｍｍ離れた位置になる。以下、特に断りのない限り、Ｔ７はリードアウト（ＲＯ）の終了位置を表すものとする。なお、リードアウト（ＲＯ）の開始と終了位置（Ｔ６およびＴ７）はＣＤ－Ｒ１に記録するデータの量に応じて変化する。上記の実際値（Ｔ６＝５８ｍｍ、Ｔ７＝５８．５ｍｍ）は記憶データ量を最大にしたときのものである。

【００２０】図２は、ＣＤ－Ｒ１の断面構造図である。ＣＤ－Ｒ１は、透明で耐熱性、耐湿性および成形性に優れ、且つ、所要の光学的特性（屈折率や複屈折など）を備えた材料（例えばプラスチック）からなる基板１ｂの上に、有機色素からなる記録層１ｃ、アルミニウムなどの金属材料からなる反射層１ｄおよび樹脂等の硬質材料からなる保護層１ｅを積層して形成されており、断面全体の厚さは１．２ｍｍである。

【００２１】ＣＤ－ＲＯＭとの構造上の相違は、記録層１ｃを有する点、および記録層１ｃと基板１ｂとの間にウォッブルグルーブと呼ばれる渦巻状の案内溝１ｆが形成されている点にある。ＣＤ－Ｒ１へのデータの記録は基板１ｂの裏側から案内溝１ｆに沿って記録用の強いレーザを照射し、記録層１ｃを加熱して情報ピット（pit：再生用のレーザ反射光を変調するための物理的変形変質部分）を形成することにより行われる。

【００２２】図３は、ＣＤ－Ｒ１の各記録領域のフォーマット概念図である。この図において、ＰＣＡ、ＰＭＡ、リードイン（ＲＩ）、データエリア（ＵＡ）およびリードアウト（ＲＯ）はそれぞれ、図１（ｂ）における同名部分に対応する。ＰＣＡおよびＰＭＡのサイズ（情報書き込み可能容量）は製造者ごとに異なり、一定ではないが、上述の試し書き回数（一般に１００回程度）やセッション情報の一時記憶回数に見合った必要量、例えば、ＰＣＡで約３．５Ｍバイト程度、ＰＭＡで約２Ｍバイト程度の容量が確保されている。ちなみに、これらの例示容量からＰＣＡの開始位置（Ｔ２）とＰＭＡの開始位置（Ｔ３）は、規格化されたリードイン（ＲＩ）の開始位置（Ｔ４）を基準として、「Ｔ２＝Ｔ４－約３５秒」の位置、「Ｔ３＝Ｔ４－約１３秒」の位置と書き表すことができる。

【００２３】既述のとおり、ＰＣＡはデータ記録を行う際の試し書き領域、ＰＭＡはクローズされていないセッション情報を一時的に格納する領域であり、これら二つの領域（ＰＣＡ／ＰＭＡ）はデータ記録時にのみ利用（アクセス）される領域である。一方、リードイン（ＲＩ）はクローズされたセッション情報をＴＯＣとして記録する領域、データエリア（ＵＡ）は実際にデータが書

き込まれる領域、リードアウト（ＲＯ）はデータエリアの終わりを明示する領域であり、これら三つの領域（リードイン／データエリア／リードアウト）はデータ記録時と再生時の両方で利用（アクセス）される領域である。

【００２４】他方、これらすべての領域をユーザからのアクセス容易性の点で見ると、すなわち、ＣＤ－Ｒ１の読み取り装置を備えたパーソナルコンピュータ等の利用者からその記憶内容を通常のツール（典型的には当該パーソナルコンピュータに搭載されたオペレーティングシステム上のファイルシステムなど）を用いて容易にアクセスできるか否かの点で評価すると、データエリア（ＵＡ）については当然ながらその記憶内容の全容把握は可能であるが、他の領域（ＰＣＡ、ＰＭＡ、リードインおよびリードアウト）の内容把握は不可能である。

【００２５】もちろん、特殊なツールを使用すれば可能ではあるが、そのようなツールは一般のユーザにとって入手困難であるから、かかる例外的なツールの利用を除けば、データエリア以外の他の領域（ＰＣＡ、ＰＭＡ、リードインおよびリードアウト）は、システムからのアクセスだけが許可された特殊な領域であるということができる。以下、この特殊領域のことを「システム領域」といい、ユーザからのアクセスが許可された領域のことを「ユーザ領域」ということにする。すなわち、データエリア（ＵＡ）はユーザ領域、それ以外のＰＣＡ、ＰＭＡ、リードイン（ＲＩ）およびリードアウト（ＲＯ）はシステム領域である。

【００２６】さて、本実施の形態におけるＣＤ－Ｒ１の特徴は、製造時に、システム領域の一部にＣＤ－Ｒ１の固有情報（以下「ＩＤ情報」という。）と所定の暗号鍵情報を書き込む点にある。ＩＤ情報はＣＤ－Ｒ１の全製造数にわたってユニークな値（重複しない値）を持つことが望ましいが、製造数が膨大になる場合、情報ビットが多ビット化してシステム領域の記憶容量を圧迫する懸念があるため、例えば、製造ロットごとや製造ラインごとまたは製造時期ごとに異なる情報としてもよい。

【００２７】このＩＤ情報は、後述するように、ユーザ段階でのＣＤ－Ｒ１へのアクセス照合に用いられる。データの再生を行うアプリケーションでＩＤの入力を要求し、入力されたＩＤとシステム領域に書き込まれているＩＤとの一致を判定して、一致の場合のみアクセスを許可する。これにより、不正なユーザ（ＩＤを知らないユーザ）によるデータの再生や複製を阻止し、データの流出や不正生成物の出現を回避することができる。

【００２８】一方、システム領域に一緒に書き込まれる鍵情報は、ユーザ段階でデータエリアに書き込まれる生データを暗号化するために用いられる。すなわち、データの記録を行うアプリケーションで暗号鍵を読み出し、この暗号鍵を用いて生データを暗号化データに変換した後、その暗号化データをＣＤ－Ｒ１のデータエリアに書き込む。この暗号鍵は暗号化データを復号する際にも用いられる。すなわち、データの再生時に、データの再生を行うアプリケーションでＩＤの入力を要求し、入力されたＩＤとシステム領域に書き込まれているＩＤとの一致を判定して、一致の場合に暗号鍵と暗号化データを読み出し、その暗号鍵を用いて暗号化データを復号し、生データに変換してユーザの利用に供する。

【００２９】したがって、ＩＤを知らない不正なユーザは、データへのアクセス自体を拒否されるから、不正なデータの読み取りを回避できると共に、万が一、何らかの手段でアクセスが成功したとしても、システム領域に書き込まれた暗号鍵へのアクセスは通常の技術知識では不可能であるから、暗号化データを生データに復号することができず、この点において万全の保全策を講じることができる。

【００３０】図４は、製造時にシステム領域に書き込まれるＩＤ情報と暗号鍵を含むデータフォーマットの例示構造図である。この図において、第一の例（ａ）は、８バイトのＩＤ情報、８バイトのＤＥＳ（Data Encryption Standard：アメリカ連邦政府標準暗号規格）暗号鍵、２バイトの製造年、１バイトの製造月および１バイトの製造日の各情報から構成された全部で２０バイトの大きさを有している。また、第二の例（ｂ）は、８バイトのＩＤ情報、２４バイトのトリプルＤＥＳ暗号鍵、２バイトの製造年、１バイトの製造月および１バイトの製造日の各情報から構成された全部で３６バイトの大きさを有している。

【００３１】いずれのフォーマットを採用するかは、もっぱら暗号鍵の信頼性を重視するか、または、システム領域の記憶容量圧迫を回避するかで決まる。なお、図示のバイト数や暗号鍵の種類およびフォーマット構造はあくまでも例示である。要はＣＤ－Ｒ１の固体識別が可能な情報（ＩＤ情報）と、生データを暗号化データに変換できる共に暗号化データから生データに復号できる所定のキー情報（暗号鍵）とを製造時にＣＤ－Ｒ１のシステム領域に書き込んでおけばよい。

【００３２】図５は、ライトワンス型光ディスク記録再生装置（以下「ＣＤ－Ｒ記録再生装置」という。）の概略的なブロック構成図である。このＣＤ－Ｒ記録再生装置１０は、ＣＤ－Ｒ１のクランピングエリア（図１（ａ）のＴ１～Ｔ２の間に設けられた情報非記録エリア）を担持して所定方向に回転駆動するスピンドルモータ１２と、ＣＤ－Ｒ１の基板１ｂを透して記録層１ｃに記録用または再生用のレーザ（一般に波長７７０～８３０ｎｍの赤外レーザ）１３を照射する光ピックアップ１４と、光ピックアップ１４の内部に設けられた不図示のシークモータと協調して光ピックアップ１４をディスクの半径方向に移動させる粗動モータ１５とを備えると共に、スピンドルモータ１２の回転速度を制御するディスク回転制御部１６と、粗動モータ１５の回転速度と回転

方向を制御する粗動モータ制御部１７と、光ピックアップ１４の位置やレーザ強度の制御を行うピックアップ制御部１８と、光ピックアップ１４からの読み取り信号や光ピックアップ１４への書き込み信号の波形変換等の制御を行う再生／記録制御部１９とを備え、さらに、これらの各制御部を統括するコントローラ２０を備える。このコントローラ２０は、発明の要旨に記載のアクセス手段、認証手段および許容手段に相当する。

【００３３】ＣＤ－Ｒ記録再生装置１０は、パーソナルコンピュータ等のホスト装置２１の拡張スロットに内蔵され（または外付けされ）、ホスト装置２１とコントローラ２０との間を所定の信号規格（例えば、ＳＣＳＩ：Small Computer System Interface）のケーブル２１ａで接続して用いられる。

【００３４】このような構成を有するＣＤ－Ｒ記録再生装置１０は、以下に示すとおり、ＣＤ－Ｒ１への情報の記録とその記録情報の再生を行うことができる。なお、ＣＤ－Ｒ１はＣＤ－ＲＯＭコンパチのデバイスであり、ＣＤ－Ｒ記録再生装置１０は、ＣＤ－ＲＯＭの情報再生も可能であるが、本発明とは直接の関連がないため説明を省略する。

【００３５】＜ＣＤ－Ｒ１への情報の記録動作＞ホスト装置２１でＣＤ－Ｒ記録専用アプリケーションプログラム（以下「ＡＰ」と省略する。）を実行すると、まず、ＡＰからのレーザ強度キャリブレーションコマンドがコントローラ２０に伝えられる。コントローラ２０はこのコマンドに応答して各制御部に所要の指令を伝え、光ピックアップ１４をＣＤ－Ｒ１のＰＣＡ空領域（試し書きされていない領域）に位置させると共に、スピンドルモータ１２の回転速度を制御（光ピックアップ１４の現在位置における相対速度が所定速度となるように制御）した後、光ピックアップ１４から暫定強度（５．５～８ｍＷの間の任意パワー）の記録用レーザ１３をＰＣＡ空領域に照射して試し書きを行う。

【００３６】次いで、コントローラ２０は、再生記録制御部１９を介してＰＣＡに試し書きされたデータを読み取り、そのデータをホスト装置２１のＡＰに返送する。ＡＰは、試し書きデータと期待値とを比較してレーザ強度の適否を判定し、判定結果が“否”であればレーザ強度を増減調節して再びレーザ強度キャリブレーションコマンドを発行する一方、判定結果が“適”であれば、ＣＤ－Ｒ１への情報の記録動作を開始する。

【００３７】この記録動作は、ユーザによって適宜に選択された所要の記録データをＡＰからコントローラ２０に伝え、このコントローラ２０の制御の下、各制御部を介してスピンドルモータ１２の回転制御および光ピックアップ１４の位置制御を行いつつ、上記記録データで光ピックアップ１４からの記録用レーザ１３を変調しながらＣＤ－Ｒ１のデータエリアに記録を行っていくというものである。そして、記録を完了すると、すべてのセッションを閉じ、そのセッション情報のＴＯＣをリードイン（ＲＩ）に書き込むと共に、最終セッションの後にリードアウト（ＲＯ）を形成する。

【００３８】＜ＣＤ－Ｒ１の記録情報の再生動作＞ＣＤ－Ｒ１の記録情報を再生する際に上記ＡＰ（ＣＤ－Ｒ記録専用アプリケーションプログラム）は不要である。但し、ＣＤ－Ｒ１のファイルシステムとホスト装置２１のファイルシステムとの相互変換を行うためのドライバソフトは必須である。ユーザはこのドライバソフトを介してＣＤ－Ｒ記録再生装置１０を利用することにより、ホスト装置２１に装備されたハードディスク等の他の記憶デバイスとの区別を意識せずにＣＤ－Ｒ１のファイルシステムにアクセスすることができる。すなわち、ユーザにはオペレーティングシステムのファイルシステムによって認識されたファイル構造が見えるから、ユーザは、他の記憶デバイスに格納されたファイルと同様の手順でＣＤ－Ｒ１内の目的とするファイルを選択し、そのファイルをコピーして他の記憶デバイスに貼り付けたり、またはＥＸＥ形式等の実行ファイルの場合は当該ファイルをオープンして実行したりすることができる。

【００３９】ＣＤ－Ｒ記録再生装置１０は、このファイルアクセスに際して、リードイン（ＲＩ）内のＴＯＣ情報を読み出してホスト装置２１のドライバソフトに提供すると共に、当該ドライバソフトから特定ファイルの読み出しコマンドを受け取った場合は、リードイン（ＲＩ）内のＴＯＣ情報を参照して当該ファイルのデータが書き込まれたデータエリア（ＵＡ）のトラックを特定し、そのトラックの開始位置に光ピックアップ１４を位置させると共に、スピンドルモータ１２の回転速度を制御し、光ピックアップ１４から再生用のレーザ（パワーが０．２ｍＷ程度に抑えられる点を除き記録用のレーザと同じもの）１３をＣＤ－Ｒ１に照射して当該ファイルデータを読み取り、その読み取りデータをホスト装置２１に転送するという一連の動作を実行する。

【００４０】以上のとおり、本実施の形態のＣＤ－Ｒ記録再生装置１０は、ＣＤ－Ｒ１への情報の書き込みを行うことができると共に、ＣＤ－Ｒ１に書き込まれた情報の再生も行うことができる。このＣＤ－Ｒ記録再生装置１０は、ユーザ段階でＣＤ－Ｒ１への情報の書き込みを行う場合に必要不可欠な構成要素であるが、ユーザ段階で、ＣＤ－Ｒ１に書き込まれた情報の再生を行う場合も必要とされる構成要素である。ＣＤ－Ｒ１はＣＤ－ＲＯＭコンパチのデバイスで、昨今のパーソナルコンピュータ等のほとんどにはＣＤ－ＲＯＭ再生装置が搭載されており、そのＣＤ－ＲＯＭ再生装置を利用してＣＤ－Ｒ１の情報再生を行うことも可能であるが、このＣＤ－ＲＯＭ再生装置は、ＣＤ－Ｒ１のシステム領域にあらかじめ書き込まれたＩＤ情報や暗号鍵にアクセスできないから、やはり、ＣＤ－Ｒ１に書き込まれた情報の再生を行う場合もＣＤ－Ｒ記録再生装置１０は欠かせない構成要

素である。

【００４１】また、ＣＤ－Ｒ記録再生装置１０はもっぱらユーザ段階で使用される装置であるが、ＣＤ－Ｒ１への情報書き込み機能に注目すると、その基本的動作は、ＣＤ－Ｒ１の製造段階で行われるＩＤ情報や暗号鍵の書き込みにも適用可能であるから、以下の説明では上記のＣＤ－Ｒ記録再生装置１０をユーザ段階と製造段階の両方で使用されるものとして話を進める。

【００４２】＜出荷時情報記録処理＞図６は、ＣＤ－Ｒ１の製造時におけるＩＤ情報と暗号鍵の書き込み動作（以下「出荷時情報記録処理」という。）を示すフローチャートである。なお、製造時にはＣＤ－Ｒ記録再生装置１０の記録機能しか利用しないため、図示のフローチャートでは、ＣＤ－Ｒ記録再生装置１０のことを便宜的に「記録機」と略称している。但し、この用語（記録機）には、ＣＤ－Ｒ記録再生装置１０に限らず、製造段階専用の“記録機”であってもよい旨の意図も含まれている。

【００４３】図において、出荷時情報記録処理を開始すると、まず、未記録のＣＤ－Ｒ１（フロー中では「ディスク」と称する。）を用意し、このＣＤ－Ｒ１を記録機に装填する（ステップＳ１１）。次に、ホスト装置２１を操作してＣＤ－Ｒ１への記録情報を手入力または自動生成する（ステップＳ１２）。この記録情報はＣＤ－Ｒ１のＩＤ情報や所定の秘密鍵および当日の日付（作成日付）などであり、そのフォーマットは、図４（ａ）または（ｂ）に示すとおりである。

【００４４】次いで、ホスト装置２１から記録機に対して情報記録命令を発行すると（ステップＳ１３）、記録機はこの命令に応答してレーザ強度キャリブレーション処理を実行し、適正なパワーに記録用レーザ１３を設定した後、光ピックアップ１４をＣＤ－Ｒ１の記録領域の“特定位置”に移動制御する（ステップＳ１４）。この特定位置は原理的にはユーザからの直接的なアクセスが認められていない領域、すなわち、システム領域（ＰＣＡ、ＰＭＡ、リードインまたはリードアウト）の未使用領域上の任意位置である。特に好ましくは、データ再生時にその存在が無視される領域として当業者に広く認知されているＰＣＡまたはＰＭＡ上の（未使用領域上の）任意位置である。以下、説明の便宜上、上記“特定位置”をＰＣＡの未使用領域上の任意位置とする。

【００４５】次いで、記録機は、ホスト装置２１から記録情報（ステップＳ１２で生成した情報）を受け取り、その記録情報を用いて記録用レーザ１３を変調しつつ、記録用レーザ１３をＣＤ－Ｒ１の透明な基板１ｂを介して記録層１ｃの案内溝１ｆに照射し、案内溝１ｆ直下の記録層１ｃに情報ピットを形成して、前記記録情報のＣＤ－Ｒ１への書き込みを行う（ステップＳ１５）。記録情報の書き込み開始位置は、上記ステップＳ１４で実行された光ピックアップ１４の移動位置、すなわち、ＰＣＡの未使用領域上の任意位置であり、記録情報の書き込み終了位置は当該位置から記録情報のサイズ（例えば、図４のフォーマットに従えば２０バイトまたは３６バイト）に相当する分だけ離れた位置である。

【００４６】次いで、記録機は、光ピックアップ１４を上記特定位置、すなわち、ＰＣＡの未使用領域上の任意位置に移動すると共に、当該位置を再生開始位置、記録情報のサイズに相当する分だけ離れた位置を再生終了位置として、システム領域に書き込んだ記録情報の再生を行い、この再生情報をホスト装置２１に転送する。ホスト装置２１は、記録機から転送された再生データと上記記録情報とを比較照合してベリファイ検査を行い（ステップＳ１６）、両者が一致していれば正常に書き込みを行えたと判断してその旨を作業者に報知する一方、そうでなければ書き込みを失敗したと判断してその旨を作業者に報知する（ステップＳ１７）。作業者は、正常書き込み報知の場合に当該ＣＤ－Ｒ１を出荷棚へ移動し（ステップＳ１８）、書き込み失敗報知の場合に当該ＣＤ－Ｒ１を不良品棚へ移動する（ステップＳ１９）。そして、以上の処理を用意されたＣＤ－Ｒ１がなくなるまで繰り返して実行する（ステップＳ２０）。

【００４７】したがって、この「出荷時情報記録処理」によれば、未記録のＣＤ－Ｒ１のシステム領域にＩＤ情報、暗号鍵および作成日付などの隠し情報を書き込んで市場に出荷し、ユーザに届けることができる。そして、ユーザ段階で、以下に説明するデータ書き込み処理、データ再生処理またはディスクコピー処理を行う際に、上記の隠し情報を利用した本実施の形態特有の処理を実行することができる。

【００４８】＜ユーザによるデータ書き込み処理＞図７は、ユーザ段階で実行されるデータ書き込み動作（以下「ユーザによるデータ書き込み処理」という。）を示すフローチャートである。この処理では、ユーザは、前述の出荷時情報記録処理によって隠し情報が書き込まれたＣＤ－Ｒ１を市場で入手し、そのＣＤ－Ｒ１をＣＤ－Ｒ記録再生装置１０にセットして、所要のユーザデータを当該ＣＤ－Ｒ１に記録する。このユーザデータについて、とりわけ重要な点は、特定の人に対してのみ再生を許可する非公開のデータ、すなわち、秘匿を要するデータである点にある。従来、この種の秘匿を要するデータをＣＤ－Ｒに記録する場合は、例えば、所定の暗号鍵でデータを暗号化してＣＤ－Ｒに記録し、そのＣＤ－Ｒと一緒に当該暗号化データの復号鍵を収めたフロッピィディスク等の記憶媒体を配布していた。しかし、このような複数媒体の同時配布は手間がかかる上、配布先での紛失等の可能性もあり、管理が面倒であるという欠点がある。

【００４９】本実施の形態のＣＤ－Ｒ１は、一つの記憶媒体に暗号化データと、その暗号化データの復号鍵とを収めて配布するので、配布先で紛失することもなく、管

理を容易にして上記不都合を解消できるというメリットがある。

【００５０】図７において、ユーザによるデータ書き込み処理を開始すると、ＣＤ－Ｒ記録再生装置１０は、ホスト装置２１からの書き込み命令の有無を判定する（ステップＳ３１）。そして、書き込み命令があると、ホスト装置２１に対してＩＤ入力要求を発行し（ステップＳ３２）、ホスト装置２１は、画面上にＩＤ入力を促がす旨の所定のＧＵＩ（Graphical User Interface）を表示してユーザによるキーボード等からのＩＤ入力を受け付け（ステップＳ３３）、入力されたＩＤ情報をＣＤ－Ｒ記録再生装置１０に転送する。

【００５１】ＣＤ－Ｒ記録再生装置１０は、ＣＤ－Ｒ１のシステム領域に書き込まれているＩＤ情報を読み出して、ホスト装置２１から転送されたＩＤ情報との一致を判定し（ステップＳ３４）、不一致であればそのまま処理を終了する一方、一致であれば、ＣＤ－Ｒ１のシステム領域に書き込まれている暗号鍵を読み出してホスト装置２１に転送する（ステップＳ３５）。ホスト装置２１は、その暗号鍵を用いて上記ユーザデータを暗号化データに変換し（ステップＳ３６）、当該暗号化データをＣＤ－Ｒ記録再生装置１０に転送する。ＣＤ－Ｒ記録再生装置１０は、転送された暗号化データをＣＤ－Ｒ１のデータエリアに記録（ステップＳ３７）した後、処理を終了する。

【００５２】図８は、上記「ユーザによるデータ書き込み処理」のタイムランを示す図であり、図中のパーソナルコンピュータ３１は上述のホスト装置２１に相当するもの、ＣＤ－Ｒライター３２は上述のＣＤ－Ｒ記録再生装置１０に相当するもの、ＣＤ－Ｒ３３は上述のＣＤ－Ｒ１に相当するものである。

【００５３】この図において、ユーザは、ＣＤ－Ｒ３３をＣＤ－Ｒライター３２に装填すると共に、パーソナルコンピュータ３１を操作して所要の書き込み命令をＣＤ－Ｒライター３２に発行する。ＣＤ－Ｒライター３２はこの書き込み命令に応答してＩＤ要求をパーソナルコンピュータ３１に返し、パーソナルコンピュータ３１は画面上にＩＤ入力を促がす旨のＧＵＩを表示する。ユーザは、そのＧＵＩに従って所定のＩＤ情報（ＣＤ－Ｒ３３の購入時に販売員等から知らされたＩＤ情報）を入力し、パーソナルコンピュータ３１は入力されたＩＤ情報をＣＤ－Ｒライター３２に転送する。

【００５４】ＣＤ－Ｒライター３２は、ＣＤ－Ｒ３３のシステム領域にあらかじめ書き込まれているＩＤ情報を読み出し、パーソナルコンピュータ３１から転送されたＩＤ情報との一致を判定して、不一致であれば処理を中止して書き込みを拒否する一方、一致していれば、ＣＤ－Ｒ３３のシステム領域にあらかじめ書き込まれている暗号鍵を読み出してパーソナルコンピュータ３１に転送する。パーソナルコンピュータ３１は、その暗号鍵を用いてユーザデータを暗号化し、暗号化データをＣＤ－Ｒライター３２に転送する。ＣＤ－Ｒライター３２は暗号化データをＣＤ－Ｒ３３のデータエリアに記録した後、記録動作の完了をパーソナルコンピュータ３１に通知して、以上一連の「ユーザによるデータ書き込み処理」を終了する。

【００５５】したがって、この「ユーザによるデータ書き込み処理」によれば、ＣＤ－Ｒのシステム領域にあらかじめ書き込まれたＩＤ情報を用いてユーザ認証を行うことができると共に、認証ユーザ（正規ユーザ）によって行われるデータ書き込みの際に、ＣＤ－Ｒのシステム領域にあらかじめ書き込まれた暗号鍵を用いてユーザデータの暗号化を行い、その暗号化データをＣＤ－Ｒに書き込むことができる。

【００５６】その結果、ユーザは、ホスト装置を操作して書き込み対象のユーザデータの指定とＩＤ情報の入力とを行うだけでよく、当該ユーザデータの暗号化処理および暗号化データのＣＤ－Ｒへの書き込みを自動化して作業性の改善を図ることができる。

【００５７】＜ユーザによるデータ再生処理＞図９は、ユーザ段階で実行されるデータ再生動作（以下「ユーザによるデータ再生処理」という。）を示すフローチャートである。この処理では、ユーザは、前述のユーザによるデータ書き込み処理によって暗号化データが書き込まれたＣＤ－Ｒ１を入手し、そのＣＤ－Ｒ１をＣＤ－Ｒ記録再生装置１０にセットして、そのＣＤ－Ｒ１から暗号鍵と暗号化データを読み出し、暗号鍵を用いて暗号化データを復号するという一連の処理を実行する。この一連の処理において、とりわけ重要な点は、二種類のユーザが存在することにある。第一のユーザは正当なＩＤ情報を知っているユーザ（以下「正規ユーザ」という。）であり、第二のユーザは正当なＩＤ情報を知らないユーザ（以下「不正ユーザ」という。）である。

【００５８】図９において、ユーザによるデータ再生処理を開始すると、ＣＤ－Ｒ記録再生装置１０は、ホスト装置２１からの再生命令の有無を判定する（ステップＳ４１）。そして、再生命令があると、ホスト装置２１に対してＩＤ入力要求を発行し（ステップＳ４２）、ホスト装置２１は、画面上にＩＤ入力を促がす旨の所定のＧＵＩを表示してユーザによるキーボード等からのＩＤ入力を受け付け（ステップＳ４３）、入力されたＩＤ情報をＣＤ－Ｒ記録再生装置１０に転送する。

【００５９】ＣＤ－Ｒ記録再生装置１０は、ＣＤ－Ｒ１のシステム領域に書き込まれているＩＤ情報を読み出して、ホスト装置２１から転送されたＩＤ情報との一致を判定し（ステップＳ４４）、不一致であれば不正ユーザと判断してそのまま処理を終了する一方、一致であれば正規ユーザと判断して、ＣＤ－Ｒ１のシステム領域に書き込まれている暗号鍵とデータエリアに書き込まれている暗号化データとを読み出してホスト装置２１に転送す

る（ステップＳ４５）。ホスト装置２１は、その暗号鍵を用いて暗号化データを復号し、当該復号データに対する正規ユーザのアクセスを許容した後、処理を終了する。

【００６０】図１０は、上記「ユーザによるデータ再生処理」のタイムランを示す図であり、図中のパーソナルコンピュータ３１は上述のホスト装置２１に相当するもの、ＣＤ－Ｒライター３２は上述のＣＤ－Ｒ記録再生装置１０に相当するもの、ＣＤ－Ｒ３３は上述のＣＤ－Ｒ１に相当するものである。

【００６１】この図において、ユーザは、ＣＤ－Ｒ３３をＣＤ－Ｒライター３２に装填すると共に、パーソナルコンピュータ３１を操作して所要の再生命令をＣＤ－Ｒライター３２に発行する。ＣＤ－Ｒライター３２はこの再生命令に応答してＩＤ要求をパーソナルコンピュータ３１に返し、パーソナルコンピュータ３１は画面上にＩＤ入力を促がす旨のＧＵＩを表示する。ユーザは、そのＧＵＩに従って所定のＩＤ情報（ＣＤ－Ｒ３３の配布先から正当に通知されたＩＤ情報）を入力し、パーソナルコンピュータ３１は入力されたＩＤ情報をＣＤ－Ｒライター３２に転送する。

【００６２】ＣＤ－Ｒライター３２は、ＣＤ－Ｒ３３のシステム領域にあらかじめ書き込まれているＩＤ情報を読み出し、パーソナルコンピュータ３１から転送されたＩＤ情報との一致を判定して、不一致であれば不正ユーザと判断し、処理を中止して再生を拒否する一方、一致していれば正規ユーザと判断し、ＣＤ－Ｒ３３のシステム領域にあらかじめ書き込まれている暗号鍵とデータエリアに書き込まれている暗号化データとを読み出してパーソナルコンピュータ３１に転送する。パーソナルコンピュータ３１は、その暗号鍵を用いて暗号化データを復号し、正規ユーザからのアクセスを許容した後、以上一連の「ユーザによるデータ再生処理」を終了する。

【００６３】したがって、この「ユーザによるデータ再生処理」によれば、ＣＤ－Ｒのシステム領域にあらかじめ書き込まれたＩＤ情報を用いて正規ユーザと不正ユーザとを識別することができると共に、正規ユーザによってデータ再生処理が行われている場合に限り、ＣＤ－Ｒのシステム領域に書き込まれた暗号鍵とデータエリアに書き込まれた暗号化データとをホスト装置に転送し、ホスト装置で暗号化データの復号を行い、復号された生データへのアクセス（例えば、データの閲覧ないし実行等）を許容することができる。

【００６４】その結果、不正ユーザを排除してデータの再生を行うことができ、データの不正閲覧および不正実行等を防止し、以って、ＣＤ－Ｒのセキュリティ性を向上することができる。

【００６５】＜ユーザによるディスクコピー処理＞図１１は、ユーザ段階で実行されるディスクコピー動作（以下「ユーザによるディスクコピー処理」という。）を示すフローチャートである。この処理では、ユーザは、前述のユーザによるデータ書き込み処理によって暗号化データが書き込まれたＣＤ－Ｒ１を入手し、そのＣＤ－Ｒ１をＣＤ－Ｒ記録再生装置１０にセットして、そのＣＤ－Ｒ１から暗号鍵と暗号化データを読み出し、当該暗号鍵を用いて暗号化データを復号し、その復号データを別のＣＤ－Ｒ記録再生装置１０にセットされた未使用のＣＤ－Ｒに書き込む（コピーする）という一連の処理を実行する。この一連の処理においても、正当なＩＤ情報を知っている正規ユーザと正当なＩＤ情報を知らない不正ユーザの二種類のユーザが存在する。

【００６６】図１１において、ユーザによるディスクコピー処理を開始すると、コピー元のＣＤ－Ｒ１を装填したＣＤ－Ｒ記録再生装置（以下「コピー元ＣＤ－Ｒ記録再生装置」という。）１０は、ホスト装置２１からのコピー命令の有無を判定する（ステップＳ５１）。そして、コピー命令があると、ホスト装置２１に対してＩＤ入力要求を発行し（ステップＳ５２）、ホスト装置２１は、画面上にＩＤ入力を促がす旨の所定のＧＵＩを表示してユーザによるキーボード等からのＩＤ入力を受け付け（ステップＳ５３）、入力されたＩＤ情報をコピー元ＣＤ－Ｒ記録再生装置１０に転送する。

【００６７】コピー元ＣＤ－Ｒ記録再生装置１０は、ＣＤ－Ｒ１のシステム領域に書き込まれているＩＤ情報を読み出して、ホスト装置２１から転送されたＩＤ情報との一致を判定し（ステップＳ５４）、不一致であれば不正ユーザと判断してＣＤ－Ｒ１のデータエリアに書き込まれた暗号化データを読み出してホスト装置２１に転送（ステップＳ５５）する一方、一致であれば正規ユーザと判断してＣＤ－Ｒ１のシステム領域に書き込まれているＩＤ情報と暗号鍵およびデータエリアに書き込まれている暗号化データを読み出してホスト装置２１に転送する（ステップＳ５６）。

【００６８】ホスト装置２１は、その転送データにＩＤ情報と暗号鍵が含まれているか否かを判定し、ＩＤ情報と暗号鍵が含まれていればそのＩＤ情報と暗号鍵および暗号化データを順次にコピー先のＣＤ－Ｒ記録再生装置１０（以下「コピー先ＣＤ－Ｒ記録再生装置」という。）１０に転送し、または、ＩＤ情報と暗号鍵が含まれていなければ転送データ（暗号化データ）それ自体をコピー先ＣＤ－Ｒ記録再生装置１０に転送する。

【００６９】コピー先ＣＤ－Ｒ記録再生装置１０は、転送されたデータにＩＤ情報と鍵情報が含まれている場合、前述の「出荷時情報記録処理」（図６参照）と同様の手順で、そのＩＤ情報と鍵情報をコピー先のＣＤ－Ｒに記録した後、暗号化データをコピー先のＣＤ－Ｒのデータエリアに記録し、または、転送されたデータにＩＤ情報と鍵情報が含まれていない場合は、暗号化データをコピー先のＣＤ－Ｒのデータエリアに記録した後、記録完了をホスト装置２１に通知して一連のディスクコピー

処理を終了する。

【００７０】図１２は、上記「ユーザによるディスクコピー処理」のタイムランを示す図であり、図中のパーソナルコンピュータ３１は上述のホスト装置２１に相当するもの、左側のＣＤ－Ｒ３３ａはコピー元のＣＤ－Ｒ１に相当するもの、左側のＣＤ－Ｒライター３２ａは上述のコピー元ＣＤ－Ｒ記録再生装置１０に相当するもの、右側のＣＤ－Ｒライター３２ｂは上述のコピー先ＣＤ－Ｒ記録再生装置１０に相当するもの、右側のＣＤ－Ｒ３３ｂはコピー先のＣＤ－Ｒに相当するものである。すなわち、この例では、左側のＣＤ－Ｒ３３ａの記録情報を右側のＣＤ－Ｒ３３ｂにディスクコピーする例を示している。

【００７１】この図において、ユーザは、コピー元とコピー先のＣＤ－Ｒ３３ａ、３３ｂをそれぞれＣＤ－Ｒライター３２ａ、３２ｂに装填すると共に、パーソナルコンピュータ３１を操作して所要のコピー命令をコピー元ＣＤ－Ｒライター３２ａに発行する。コピー元ＣＤ－Ｒライター３２ａはこのコピー命令に応答してＩＤ要求をパーソナルコンピュータ３１に返し、パーソナルコンピュータ３１は画面上にＩＤ入力を促がす旨のＧＵＩを表示する。ユーザは、そのＧＵＩに従って所定のＩＤ情報（ＣＤ－Ｒ３３ａの配布先から正当に通知されたＩＤ情報）を入力し、パーソナルコンピュータ３１は入力されたＩＤ情報をコピー元ＣＤ－Ｒライター３２ａに転送する。

【００７２】コピー元ＣＤ－Ｒライター３２ａは、ＣＤ－Ｒ３３ａのシステム領域にあらかじめ書き込まれているＩＤ情報を読み出し、パーソナルコンピュータ３１から転送されたＩＤ情報との一致を判定して、不一致であれば不正ユーザと判断し、暗号化データのみの限定的コピーを許容する一方、一致していれば正規ユーザと判断し、ＣＤ－Ｒ３３ａのシステム領域にあらかじめ書き込まれているＩＤ情報と暗号鍵およびデータエリアに書き込まれている暗号化データを読み出してパーソナルコンピュータ３１に転送する。

【００７３】パーソナルコンピュータ３１は、コピー先ＣＤ－Ｒライター３２ｂに書き込み命令を発行すると共に、コピー元のＣＤ－Ｒ３３ａから読み出したＩＤ情報、暗号鍵および暗号化データをコピー先ＣＤ－Ｒライター３２ｂに転送する。コピー先ＣＤ－Ｒライター３２ｂはそのＩＤ情報と暗号鍵をＣＤ－Ｒ３３ｂのシステム領域に書き込むと共に、その暗号化データをＣＤ－Ｒ３３ｂのデータエリアに書き込み、その書き込み完了をホスト装置２１に通知して、以上一連の「ユーザによるディスクコピー処理」を終了する。

【００７４】したがって、この「ユーザによるディスクコピー処理」によれば、コピー元ＣＤ－Ｒのシステム領域にあらかじめ書き込まれたＩＤ情報を用いて正規ユーザと不正ユーザとを識別することができると共に、正規ユーザによってディスクコピー処理が行われている場合に限り、コピー元ＣＤ－Ｒのシステム領域に書き込まれたＩＤ情報と暗号鍵およびデータエリアに書き込まれた暗号化データをホスト装置に転送し、ホスト装置からコピー先ＣＤ－Ｒライターに転送して、コピー先ＣＤ－Ｒに書き込む（コピーする）ことができる。

【００７５】その結果、正規ユーザだけにディスクコピーを許可してコピー元ＣＤ－Ｒの完全副生物を製造させることができる一方、不正ユーザに対しては暗号化データのみの限定的コピーを許可し、実質的に再利用不能（暗号を解読しない限りデータを利用できない）な未完成副生物を製造させることができ、海賊版ＣＤ等の不正複製物の出現を防止して、ＣＤ－Ｒのセキュリティ性の向上を図ることができる。

【００７６】＜まとめ＞以上、説明したとおり、本実施の形態のＣＤ－Ｒ１は、ユーザによる直接的なアクセスが認められていない特定の領域（システム領域）にＩＤ情報や暗号鍵といった隠し情報を書き込んで出荷するから、ユーザ段階のデータ書き込みやデータ再生の際に用いられるＣＤ－Ｒライター（ＣＤ－Ｒ記録再生装置１０）に、その隠し情報を利用したセキュリティ機能を実装しておくことにより、ＣＤ－Ｒ１へのアクセス権限の認証を行うことが可能となり、正規ユーザに対してのみデータ書き込みやデータ再生を許可することができる。

【００７７】したがって、ライトワンス型の特徴（データの消去や改ざんが不可能）に加えて、さらに、積極的なセキュリティ性を持たせたＣＤ－Ｒ１を市場に提供することができ、特に秘匿を要するデータの保管や配布の分野に適用してきわめて好ましいライトワンス型光ディスクを実現できるという社会的有益性を奏することができる。

【００７８】なお、以上の説明では、ＩＤ情報や暗号鍵などの隠し情報をシステム領域に書き込んでいるが、このシステム領域とは、ユーザによる直接的なアクセスが許容された領域（典型的にはデータエリア）以外の領域という意味であり、前述のＰＣＡやＰＭＡはもちろんのこと、リードインであってもよいし、リードアウトであってもよく、あるいは、これ以外の領域が存在するならば、その領域であってもよい。

【００７９】また、暗号鍵については、特に説明を加えなかったが、一般的に知られている様々な暗号化方式（例えば、前述のＤＥＳ方式以外にも、ＦＥＡＬ：Fast Encipherment Algorithmなどの方式がある。）のいずれを採用してもかまわない。解読の困難性、暗号化処理や復号処理のオーバヘッドおよび暗号化データのボリューム等を勘案して適切な方式を採用すればよい。

【００８０】また、前記説明のＩＤ情報や暗号鍵を利用したセキュリティ機能は、もっぱらＣＤ－Ｒ記録再生装置１０のコントローラ２０やホスト装置２１のメインボードに実装されたマイクロコンピュータならびに各種周

辺機器を含むハードウェア資産と、オペレーティングシステムや各種プログラム（ドライバソフトを含む）などのソフトウェア資産との有機的結合によって機能的に実現されるものであるが、ハードウェア資産およびオペレーティングシステムは汎用のものを利用できるから、前記説明のＩＤ情報や暗号鍵を利用したセキュリティ機能にとって欠くことのできない必須の事項は、実質的に、前述の「ユーザによるデータ書き込み処理」（図７参照）、「ユーザによるデータ再生処理」（図９参照）および「ユーザによるディスクコピー処理」（図１１参照）などのプログラムに集約されているということがいえる。

【００８１】したがって、本発明に係るＩＤ情報や暗号鍵を利用したセキュリティ機能は、それらのプログラムのすべてまたはその要部を格納した、フロッピィディスク、光ディスク、コンパクトディスク、磁気テープ、ハードディスクまたは半導体メモリなどの記録媒体若しくはこれらの記録媒体を含む構成品（ユニット品や完成品または半完成品）を包含する。なお、その記録媒体または構成品は、それ自体が流通経路にのるものはもちろんのこと、ネットワーク上にあって記録内容だけを提供するものも含まれる。

【００８２】また、以上の説明では、ライトワンス型光ディスクとしてＣＤ－Ｒの例を示したが、これに限らない。例えば、ＤＶＤ（Digital Video DiscまたはDigital Versatile Disc）－Ｒも１回だけのデータ書き込みを行うことができるから、もちろんライトワンス型光ディスクの仲間である。上記説明をＤＶＤ－Ｒに適用する場合、ＣＤ－ＲをＤＶＤ－Ｒと読み替えると共に、ＣＤ－Ｒ記録再生装置やＣＤ－Ｒライターをそれぞれ ＤＶＤ－Ｒ記録再生装置、ＤＶＤ－Ｒライターと読み替えればよい。

【００８３】

【発明の効果】請求項１記載の発明によれば、システム領域に書き込まれたセキュリティ対策のための情報がユーザからの不可視状態を保って出荷されるため、当該情報をユーザからの隠し情報とすることができる。

【００８４】請求項２記載の発明によれば、データの再生時にその存在が無視される特定の領域（レーザ強度キャリブレーション用領域）にセキュリティ対策のための情報が書き込まれて出荷される。当該領域はユーザに対して不可視であるばかりか、当業者にとってもレーザ強度キャリブレーション用として広く理解されているため、かかる専門知識を有する当業者に対しても不可視性を確保することができる。

【００８５】請求項３記載の発明によれば、いずれもユーザからの直接的なアクセスが許容されていない領域にセキュリティ対策のための情報が書き込まれて出荷される。したがって、当該情報をユーザからの隠し情報とすることができる。

【００８６】請求項４記載の発明によれば、ユーザ段階で、セキュリティ対策のための情報を利用したユーザ認証が可能となる。したがって、かかる認証結果を用いて不正ユーザを排除でき、データの記録や再生時のセキュリティを向上することができる。

【００８７】請求項５記載の発明によれば、ユーザ段階で、セキュリティ対策のための情報を利用したユーザデータの暗号化が可能となる。したがって、万が一不正認証された場合でも、生データが露呈しないため、データの秘匿性を確保することができる。

【００８８】請求項６記載の発明によれば、ユーザ段階で、セキュリティ対策のための情報を利用した暗号化データの復号が可能となる。したがって、万が一不正認証された場合でも、セキュリティ対策のための情報が読み取られない限り、生データが露呈せず、データの秘匿性を確保することができる。

【００８９】請求項７記載の発明によれば、システム領域の一部にセキュリティ対策のための情報が書き込まれたライトワンス型光ディスクを装填して、そのセキュリティ対策のための情報を利用することにより、正規ユーザの認証処理が可能となり、例えば、前記ライトワンス型光ディスクへのデータ記録や、前記ライトワンス型光ディスクからのデータ再生の際のセキュリティを確保できる。したがって、ライトワンス型光ディスクの特徴（データの消去や改ざんが不可能）に加えて、より積極的なデータ保全策を講じることができ、特に秘匿を要するデータの保管や配布の分野に用いて好適なライトワンス型光ディスク用記録再生装置を提供できる。

【００９０】請求項８記載の発明によれば、マイクロコンピュータを含むハードウェア資産と該プログラムとの有機的結合によって前記アクセス手段、認証手段および許容手段を実現することができる。

【図面の簡単な説明】

【図１】ライトワンス型光ディスクの外観図およびその要部拡大図である。

【図２】ＣＤ－Ｒの断面構造図である。

【図３】ＣＤ－Ｒの各記録領域のフォーマット概念図である。

【図４】製造時にシステム領域に書き込まれるＩＤ情報と暗号鍵を含むデータフォーマットの例示構造図である。

【図５】ライトワンス型光ディスク記録再生装置の概略的なブロック構成図である。

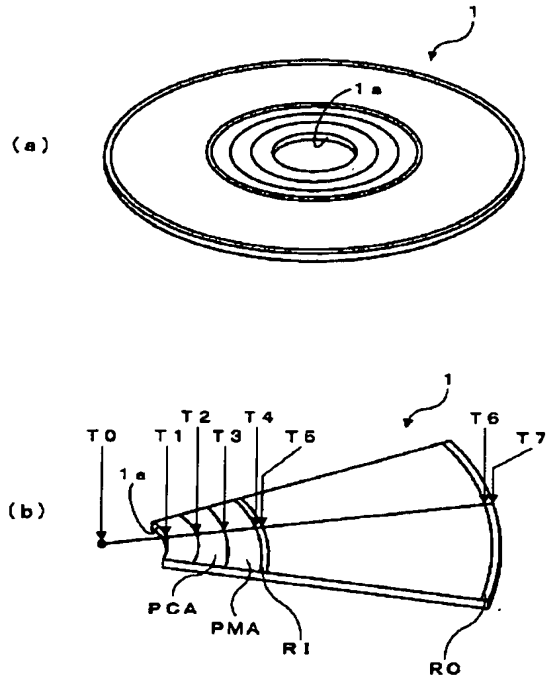
【図６】ＣＤ－Ｒの製造時におけるＩＤ情報と暗号鍵の書き込み動作（出荷時情報記録処理）を示すフローチャートである。

【図７】ユーザ段階で実行されるデータ書き込み動作（ユーザによるデータ書き込み処理）を示すフローチャートである。

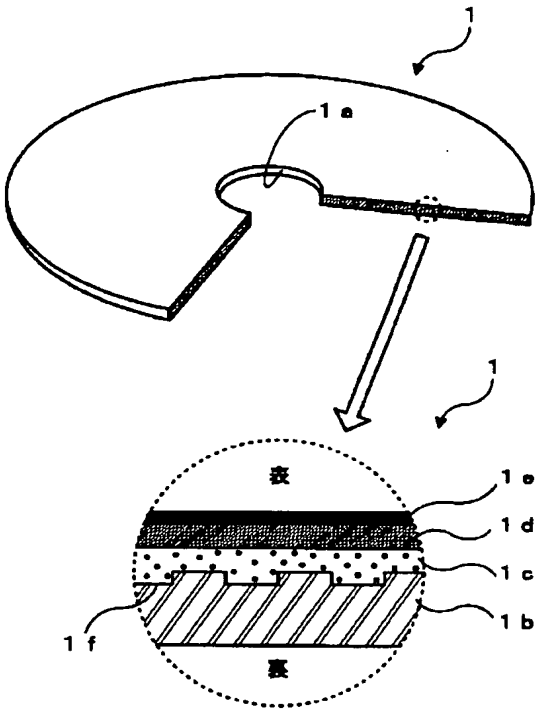
【図８】ユーザによるデータ書き込み処理のタイムラン

を示す図である。
【図９】ユーザ段階で実行されるデータ再生動作（ユーザによるデータ再生処理）を示すフローチャートである。
【図１０】ユーザによるデータ再生処理のタイムランを示す図である。
【図１１】ユーザ段階で実行されるディスクコピー動作（ユーザによるディスクコピー処理）を示すフローチャートである。
【図１２】ユーザによるディスクコピー処理のタイムランを示す図である。
【符号の説明】
ＰＣＡ　Power Calibration Area（システム領域、レーザ強度キャリブレーション用領域）
ＰＭＡ　Program Memory Area（システム領域、セッション情報の一時格納用領域）
ＲＩ　リードイン（セッション情報格納用領域）
ＲＯ　リードアウト（ユーザ領域の終了位置を明示するための領域）
ＵＡ　ユーザエリア（ユーザ領域）
１　ＣＤ－Ｒ（ライトワンス型光ディスク）
１０　ＣＤ－Ｒ記録再生装置（ライトワンス型光ディスク用記録再生装置）
２０　コントローラ（アクセス手段、認証手段、許容手段）

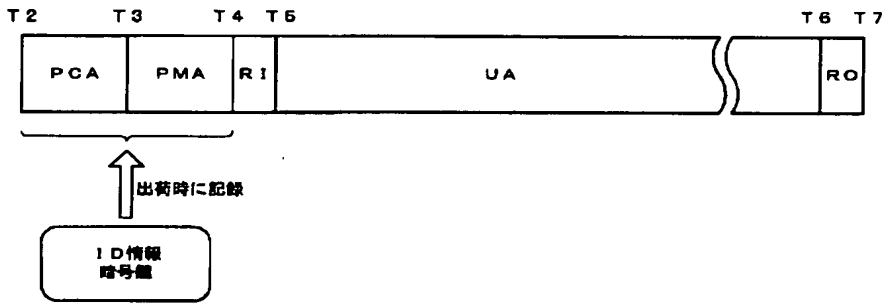
【図１】



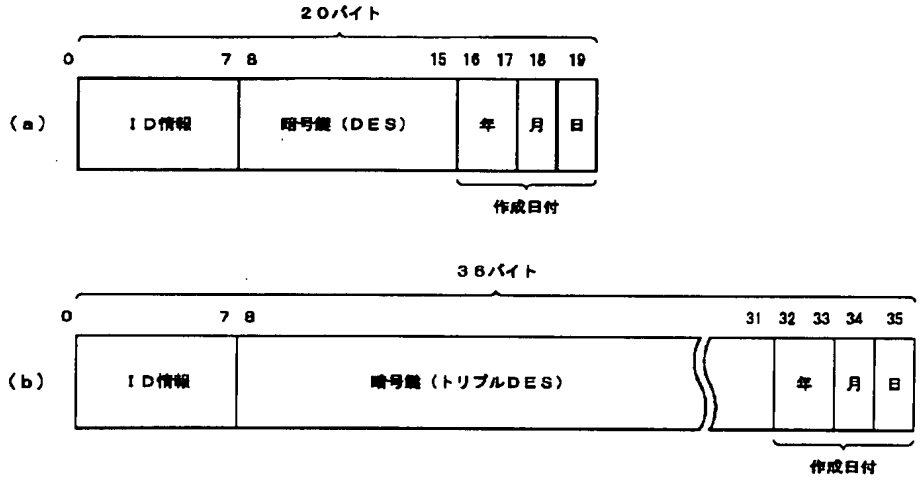

【図２】



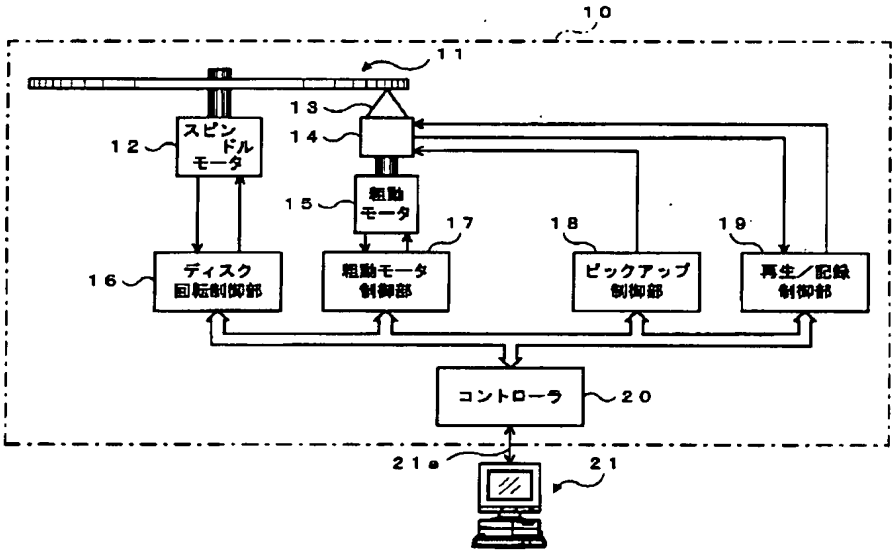

【図３】



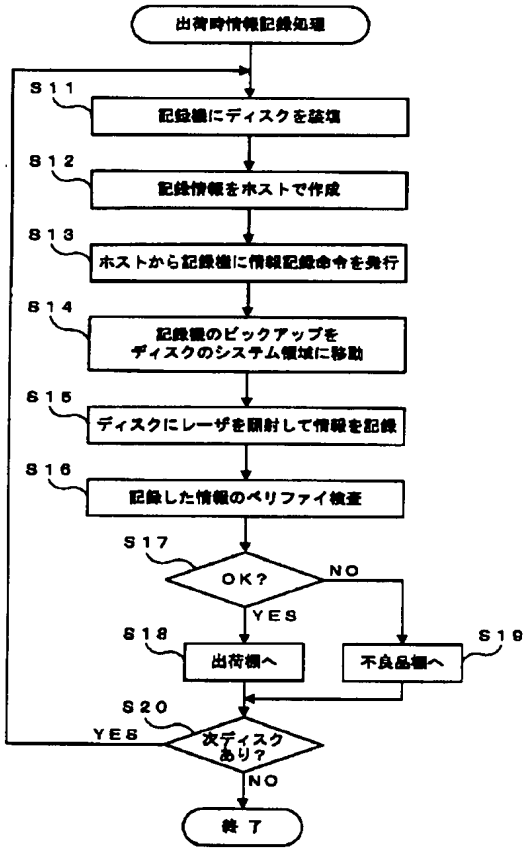
【図４】


２０バイト
0
7 8
15 16 17 18 19
(a)
ＩＤ情報
暗号鍵（ＤＥＳ）
年
月
日
作成日付
３６バイト
0
7 8
31 32 33 34 35
(b)
ＩＤ情報
暗号鍵（トリプルＤＥＳ）
年
月
日
作成日付

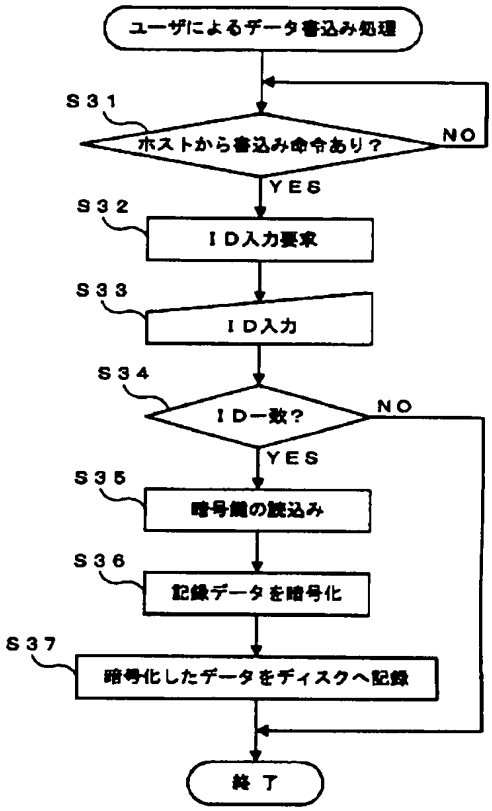
【図５】


10
11
13
14
12
スピンドルモータ
15
粗動モータ
17
18
19
16
ディスク回転制御部
粗動モータ制御部
ピックアップ制御部
再生／記録制御部
コントローラ
20
21a
21

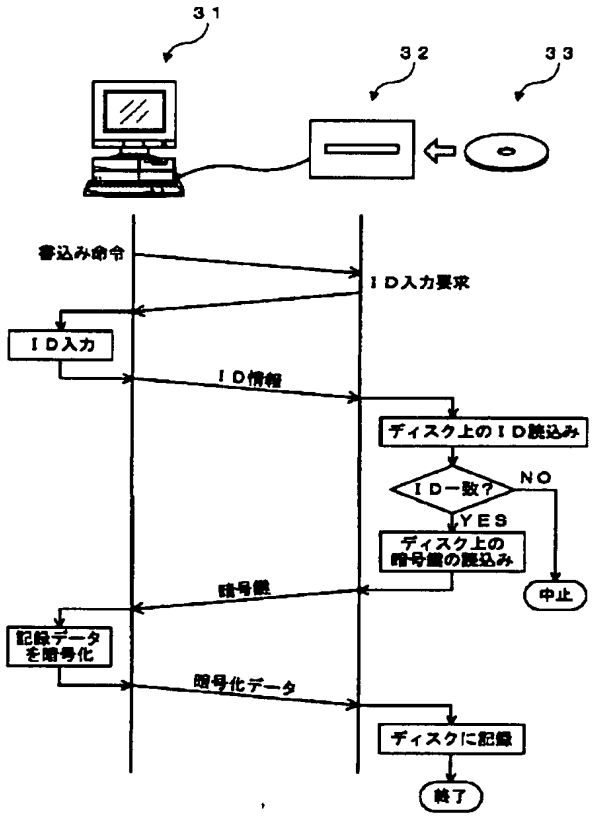
【図６】


出荷時情報記録処理
S11
記録機にディスクを装填
S12
記録情報をホストで作成
S13
ホストから記録機に情報記録命令を発行
S14
記録機のピックアップを
ディスクのシステム領域に移動
S15
ディスクにレーザを照射して情報を記録
S16
記録した情報のベリファイ検査
S17
OK?
NO
YES
S18
出荷棚へ
S19
不良品棚へ
S20
次ディスク
あり?
YES
NO
終了

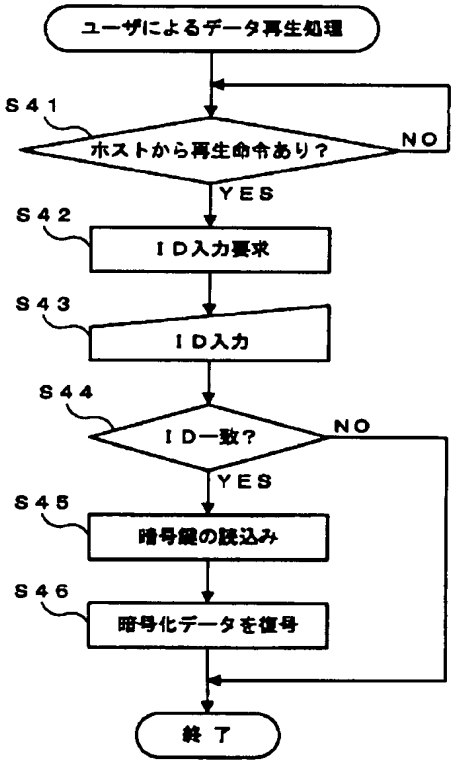
【図７】


ユーザによるデータ書込み処理
S31
ホストから書込み命令あり?
NO
YES
S32
ＩＤ入力要求
S33
ＩＤ入力
S34
ＩＤ一致?
NO
YES
S35
暗号鍵の読込み
S36
記録データを暗号化
S37
暗号化したデータをディスクへ記録
終了

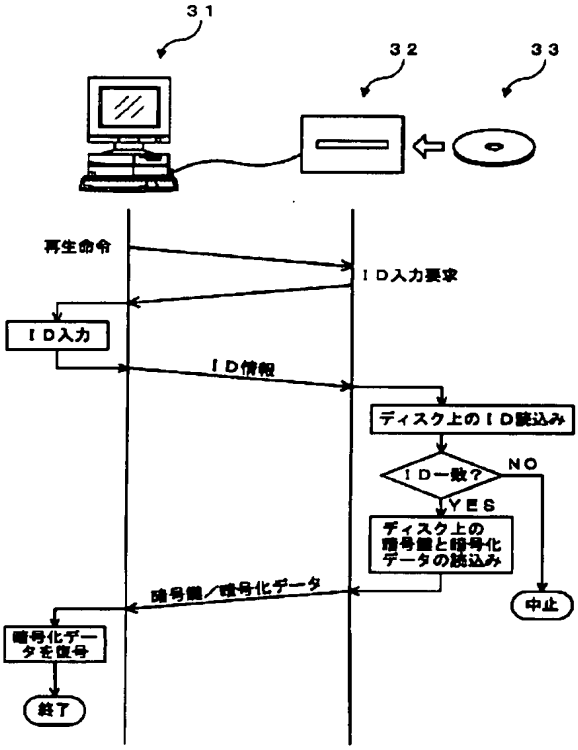
【図８】


31
32
33
書込み命令
ＩＤ入力要求
ＩＤ入力
ＩＤ情報
ディスク上のＩＤ読込み
ＩＤ一致？
NO
YES
ディスク上の暗号鍵の読込み
中止
暗号鍵
記録データを暗号化
暗号化データ
ディスクに記録
終了

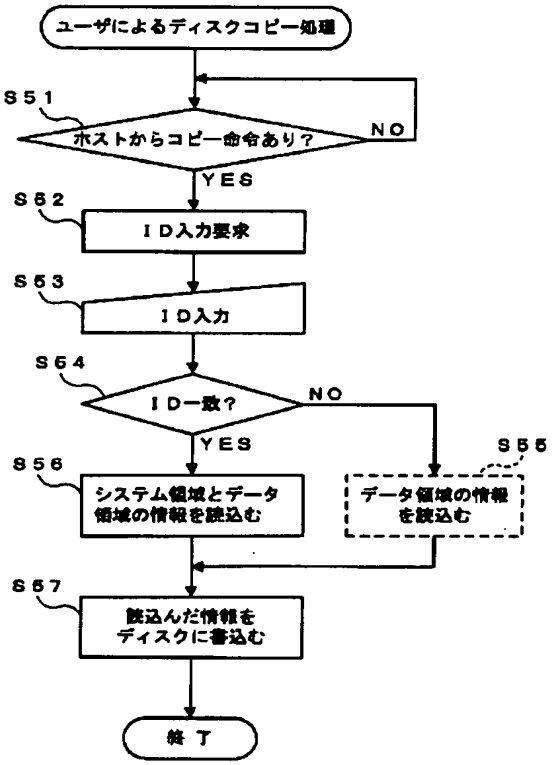
【図９】


ユーザによるデータ再生処理
S41
ホストから再生命令あり？
NO
YES
S42
ＩＤ入力要求
S43
ＩＤ入力
S44
ＩＤ一致？
NO
YES
S45
暗号鍵の読込み
S46
暗号化データを復号
終了

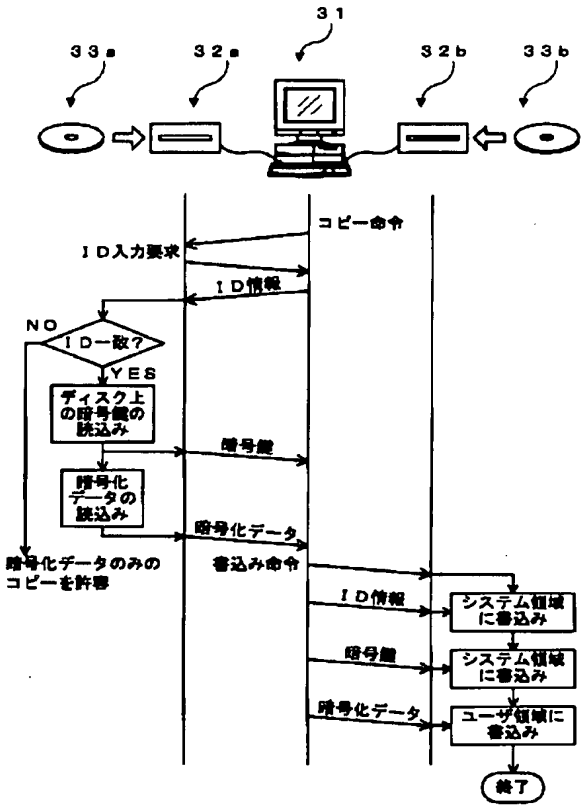
【図１０】


31
32
33
再生命令
ＩＤ入力要求
ＩＤ入力
ＩＤ情報
ディスク上のＩＤ読込み
ＩＤ一致？
NO
YES
ディスク上の暗号鍵と暗号化データの読込み
中止
暗号鍵／暗号化データ
暗号化データを復号
終了

【図１１】




【図１２】




フロントページの続き

(72)発明者　清水　洋信
東京都台東区上野６丁目16番20号　太陽誘電株式会社内

Ｆターム(参考)　5B017 AA03 BA05 BA07 CA09
5D044 BC05 CC06 DE02 DE50 DE70 GK17
5D066 DA02 DA20
5D090 AA01 BB03 CC04 DD03 FF24 FF49 GG24